ima®

The Association of Accountants and Financial Professionals in Business

Enterprise Risk Management: Tools and Techniques for Effective Implementation

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).

Enterprise Risk Management: Tools and Techniques for Effective Implementation

Table of Contents

I. Executive Summary . . . 3

II. Introduction . . . 3

III. Scope . . . 4

IV. Risk Identification Techniques . . . 6

- Brainstorming . . . 7
- Event Inventories and Loss Event Data . . . 8
- Interviews and Self-Assessment . . . 9
- Facilitated Workshops . . . 11
- SWOT Analysis . . . 12
- Risk Questionnaires and Risk Surveys . . . 12
- Scenario Analysis . . . 13
- Using Technology . . . 14
- Other Techniques . . . 14

V. Analysis of Risk by Drivers . . . 15

VI. Risk Assessment Tools . . . 17

- Categories . . . 17
- Qualitative vs. Quantitative . . . 18
- Risk Rankings . . . 19
- Impact and Probability . . . 19
- Keys to Risk Maps . . . 22
- Link to Objectives at Risk or Divisions at Risk . . . 23
- Residual Risk . . . 23
- Validating the Impact and Probability . . . 23
- Gain/Loss Curves . . . 24
- Tornado Charts . . . 25
- Risk-Adjusted Revenues . . . 25
- A Common Sense Approach to Risk Assessment . . . 26
- Probabilistic Models . . . 27
- Seemingly Nonquantifiable Risks . . . 29

VII. Practical Implementation Considerations . . . 30

- ERM Infrastructure . . . 30
- ERM Maturity Models . . . 31
- Staging ERM Adoption for Early Wins . . . 32

The Role of the Management Accountant . . . 33
ERM Education and Training . . . 33
Technology . . . 34
Aligning Corporate Culture . . . 34
The ROI of ERM . . . 35

VIII. Conclusion . . . 35

Glossary . . . 36

Additional Resources . . . 36

Table of Exhibits

Exhibit 1: COSO *Enterprise Risk Management—Integrating with Strategy and Performance* Components and Principles . . . 5

Exhibit 2: COSO *Enterprise Risk Management—Integrating with Strategy and Performance* Overview . . . 6

Exhibit 3: Industry Portfolio of Risks . . . 9

Exhibit 4A-C: Risk Identification Template . . . 10

Exhibit 4D: Risk Identification Template (cont'd) . . . 11

Exhibit 5: Influence Diagram . . . 15

Exhibit 6: Quantifying Risk—Determine the Drivers . . . 16

Exhibit 7: Linking Objectives to Strategies to Risks to KRIs . . . 17

Exhibit 8: Portfolio View of Risk . . . 18

Exhibit 9: Qualitative and Quantitative Approaches to Risk Assessment . . . 19

Exhibit 10: Risk Map . . . 20

Exhibit 11: Risk Map Model . . . 21

Exhibit 12: Illustrative Combined Risk and Opportunity Map . . . 22

Exhibit 13: Gain/Loss Probability Curve . . . 24

Exhibit 14: Tornado Chart—Earnings Variability by Sample Risks . . . 25

Exhibit 15: Actual Revenue vs. Risk-Corrected Revenue . . . 26

Exhibit 16: Goals of Risk Management . . . 26

Exhibit 17: Earnings at Risk by Risk Factor . . . 27

Exhibit 18: Earnings at Risk Hedge Effectiveness Comparisons . . . 28

Exhibit 19: Expected Earnings and EaR . . . 28

Exhibit 20: Probability Assessment of Earnings Outcome . . . 29

Exhibit 21: ERM Maturity Model . . . 31

I. Executive Summary

One of the authors' earlier studies of enterprise risk management (ERM) stated that the goal of ERM is to create, protect, and enhance shareholder value. Since then, ERM research has shown that ERM adds value and helps organizations make better decisions. ERM takes a broad perspective on identifying the risks that could cause an organization to fail to meet its strategies and objectives. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) defines ERM as, "The culture, capabilities, and practices, integrated with strategy-setting and performance, that organizations rely on to manage risk in creating, preserving, and realizing value." To meet more objectives (strategic, operational, or in other areas) more of the time, organizations must get better at managing risks. In this IMA® (Institute of Management Accountants) Statement on Management Accounting (SMA), several techniques for identifying risks are discussed and illustrated with examples from company experiences. Once risks are identified, the next issue is to determine the root causes or what drives the risks. A suggested approach is described and followed by a discussion of several qualitative and quantitative procedures for assessing risks. Some practical ERM implementation considerations are also explored, including infrastructure and maturity models, staging adoption, the role of the management accountant, education and training, technology, aligning corporate culture, building a case for ERM, and the return on investment (ROI) of ERM. Any organization—large or small; public, private, or not-for-profit; U.S.-based or global—that has a stakeholder with expectations for business success can benefit from the tools and techniques provided in this SMA.

II. Introduction

In the economic landscape of the 21st Century, an organization's business model is challenged constantly by competitors and events that could give rise to substantial risks. An organization must strive to find creative ways to continuously reinvent its business model in order to sustain growth and create value for stakeholders. Companies make money and increase stakeholder value by engaging in activities that have some risk, yet stakeholders also tend to appreciate and reward some level of stability in their expected returns. Failure to identify, assess, and manage the major risks facing the organization's business model, however, may unexpectedly result in significant loss of stakeholder value. Thus, senior leadership must implement processes to manage effectively any substantial risks confronting the organization.

While leaders of successful organizations have always had some focus on managing risks, it typically has been from a reactive exposure-by-exposure standpoint or a silo approach rather than a proactive, integrated, across-the-organization perspective. Under a silo approach, individual organizational units deal with their own risks, and often no single group or person in the organization has a grasp of the entire exposure confronting the company (especially the overall organization's "reputation" risk). To correct such a situation, enterprise risk management (ERM) has emerged in recent years and takes an integrated and holistic view of the risks facing the organization.

This Statement on Management Accounting (SMA) is the second one to address ERM. The first, *Enterprise Risk Management: Frameworks, Elements, and Integration*, serves as the foundation for understanding and implementing ERM. It highlights the various risk frameworks and statements that professional organizations around the world have published. In addition, it discusses and illustrates through company experiences the core components of a generic ERM framework. It also points out some entrepreneurial opportunities for change within an organization (with specific leadership roles for the management accountant articulated) when ERM is incorporated in such ongoing management activities such as strategic planning, the balanced scorecard (BSC), innovation, budgeting, business continuity planning, and corporate governance.

III. Scope

This SMA is addressed to management accounting and finance professionals who serve as strategic business partners with management in the implementation of ERM in their organization. Others within the organization responsible for risk management, information technology, and internal audit will also find this SMA useful.

Like many other change initiatives going on within dynamic organizations, ERM provides an opportunity for management accounting and finance professionals to alter how they are perceived by others in the organization. By becoming strategic partners in ERM implementation, they can be seen as "bean sprouters" of new management initiatives rather than merely "bean counters." They also can move from being the historians and custodians of accounts to futuristic thinkers. They can become coaches and players in a new management initiative important to the future overall well-being of the company rather than merely scorekeepers on what has or has not been accomplished.[1]

The focus of this SMA is on core tools and techniques to facilitate successful ERM implementation. While other tools and techniques can be found in the Additional Resources section at the end of this SMA, this document emphasizes those that are critical for most ERM initiatives. Since all organizations have stakeholders with ever-increasing expectations, the tools and techniques discussed here are generally relevant to:

- Large and small organizations,
- Enterprises in the manufacturing and services sectors,
- Public and private organizations, and
- For-profit and not-for-profit organizations.

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) 2017 *Enterprise Risk Management—Integrating with Strategy and Performance* framework lists the following potential benefits of ERM:

- Increase the range of opportunities by considering all possibilities.
- Increase positive outcomes.

[1] The authors acknowledge that the ideas in this paragraph about the changing role of financial professionals were taken from a presentation heard some years ago (uncertain as to date and place) and given by Jim Smith of The Marmon Group, Inc. While the original remarks were not given in the context of ERM, they have been adapted accordingly.

- Reduce negative surprises.
- Identify entity-wide risks.
- Manage entity-wide risks.
- Reduce performance variability.
- Improve resource deployment.

These are potential benefits that all management accounts are likely to want for their organizations.

One way to get many of these benefits is to adopt an ERM framework and apply ERM principles. COSO identified 20 ERM principles in its new framework. Exhibit 1 shows the 20 principles aligned under the five components.

EXHIBIT 1: COSO *ENTERPRISE RISK MANAGEMENT—INTEGRATING WITH STRATEGY AND PERFORMANCE* COMPONENTS AND PRINCIPLES

This SMA highlights many tools and techniques that align with these COSO components and help organizations implement the framework and follow the ERM principles related to the components. While this SMA is not an exhaustive list of all tools for all principles, it can be used to grow an organization's ERM maturity.

Much of this SMA helps organizations that are trying to implement the "performance" and "review and revision" components noted in Exhibit 1. For example, Sections IV, V, and VI review risk identification, analysis by drivers, and risk assessment tools. These sections will help with the principles related to identifying risk, assessing the severity of risks, prioritizing risks, responding to risks, and developing a portfolio view (again, see Exhibit 1 for these 20 ERM principles). The discussion on scenario analysis in Section IV shows one way to see how many risks might be correlated around a central risk event and is related to Principle 14. Other tools and techniques related to principles such as assessing change and improving ERM are also covered with the latter being addressed in Section VII. A few tools in this SMA are also especially helpful for ERM principles in COSO's second component related to strategy and objective setting. For example, the facilitated workshops discussion in Section IV highlights how some companies do environmental scans, black swan, and strategic disruption workshops to help understand strategic risks in the present and the future. These workshops specifically help with the ERM principles, analyzing the context and evaluating alternative strategies.

IV. Risk Identification Techniques

Exhibit 2 shows the 2017 COSO ERM framework components. The initial focus is on mission, vision, and core values, and then onto strategy development and objective setting. The focal point for risk identification may be at any level, such as the overall company, a strategic business unit, a function, a project, a process, or an activity. Without clear objectives, it is impossible to identify events that might give rise to risks that could impede the accomplishment of a particular strategy or objective—regardless of the scope of the inquiry. Assuming those involved in identifying risks have a clear understanding of the mission, vision, core values, strategies, and objectives, the appropriate questions to ask, as suggested by one company's senior enterprise risk manager, are: "What could stop us from reaching our top goals and objectives?" and "What would materially damage our ability to survive?" These questions can be modified for the appropriate level of inquiry.

EXHIBIT 2: COSO *ENTERPRISE RISK MANAGEMENT—INTEGRATING WITH STRATEGY AND PERFORMANCE* OVERVIEW

In the risk identification process, those involved should recognize that it is a misperception to think of a risk "as a sudden event."[2] Identifying an issue that is facing the organization and discussing it in advance can potentially lead to the risk being mitigated. Two benefits are possible:

> One, if you mitigate the risk and your peers do not—in a catastrophic, continuity-destroying event that hits an industry—say a financial scandal—you get what is called the survivor's bonus. Two, if you survive or survive better than others, then you have an upside after the fact, and this should be part of the board's strategic thinking.[3]

Before considering some of the specific techniques available for organizations to identify risks, several important factors should be noted about this process:

- The end result of the process should be a risk language specific to the company or the unit, function, activity, or process (whatever is the focal point);

[2] Corporate Board Member, *2006 Academic Council Supplement: Emerging Trends in Corporate Governance*, Board Member, Inc., Brentwood, Tenn., p. 20.

[3] *Ibid.*

- Clarify the actual risk vs. causes or impacts of the risk;
- Using a combination of techniques may produce a more comprehensive list of risks rather than reliance on a single method;
- The techniques used should encourage open and frank discussion, and individuals should not fear reprisal for expressing their concerns about potential events that would give rise to risks resulting in major loss to the company;
- Consider cognitive biases (such as framing) that might limit a person's ability to identify the risk correctly.
- The process should involve a cross-functional and diverse team both for the perspectives such a group provides and to build commitment to ERM; and
- Finally, the process will probably generate a lengthy list of risks, and the key is to focus on the "vital few" rather than the "trivial many."

Some techniques for identifying risk are:

- Brainstorming
- Event inventories and loss event data
- Interviews and self-assessment
- Facilitated workshops
- SWOT analysis
- Risk questionnaires and risk surveys
- Scenario analysis
- Using technology
- Other techniques

Brainstorming

When objectives are stated clearly and understood by the participants, a brainstorming session drawing on the creativity of the participants can be used to generate a list of risks. In a well-facilitated brainstorming session, the participants are collaborators, comprising a team that works together to articulate the risks that may be known by some in the group. In the session, risks that are known unknowns may emerge, and perhaps even some risks that were previously unknown unknowns may become known. Facilitating a brainstorming session takes special leadership skills, and, in some organizations, members of the internal audit and ERM staff have been trained and certified to conduct risk brainstorming sessions. The participants, in addition to well-trained facilitators, need to understand the ERM framework and how the brainstorming session fits into the ERM process. The participants may very well be required to do some preparation prior to the session.

In using this technique, one company familiar to the authors noted that because the objectives were unclear to some of the participants, the process had to be backed up and the objectives clarified before proceeding. Using a cross-functional team of employees greatly increases the value of the process because it sheds light on how risks and objectives are correlated and how they can impact business units differently. Often in brainstorming sessions

focused on risk identification, a participant may mention a risk only to have another person say: "Come to think of it, my area has that risk, and I have never thought of it before." With the team sharing experiences, coming from different backgrounds, and having different perspectives, brainstorming can be successful in identifying risk. It is also powerful when used at the executive level or with the audit committee and/or board of directors.

In a brainstorming session, the participants must have assurance that their ideas will not result in humiliation or demotion. Otherwise, they may feel inhibited in expressing what they believe are major risks facing the organization. As an example, a set of often-overlooked risks are "people risks" vs. environmental risks, financial risks, and other more technical risks. People risks include succession planning ("What if our very competent leader departs the organization?") and competency and skills building ("What if we continue with a team that does not have the requisite skills for success?"). Once a list of risks is generated, reducing the risks to what the group considers the top few can be accomplished using group software to enable participants to anonymously vote on the objectives and risks. Anonymity is believed to increase the veracity of the rankings. With the availability of interactive voting software and web polling, the brainstorming session might be conducted as a virtual meeting with participants working from their office location, also enabling them to identify and rank the risks anonymously.

Event Inventories and Loss Event Data

Seeding or providing participants with some form of stimulation on risks is very important in a brainstorming session. One possibility is to provide an event inventory for the industry (see Exhibit 3) or a generic inventory of risks. Examples of the latter are readily available from various consulting firms and publications.[4] In the first SMA on ERM, a general risk classification scheme is given that could also be used to "seed" the discussion. In a brainstorming session or facilitated workshop (discussed later in this section), the goal is to reduce the event inventory to those relevant to the company and define each risk specific to the company. The risk identification process can also be seeded by available loss event data. A database on relevant loss events for a specific industry can stimulate a "fact-based discussion."[5] COSO's 2017 ERM framework specifically notes that data tracking can be a valuable risk identification technique. The data to be tracked can be based on historical data or purchased from service providers.

[4] Economist Intelligence Unit, *Managing Business Risks—An Integrated Approach,* The Economist Intelligent Unit, New York, N.Y., 1995.

[5] COSO, *Enterprise Risk Management—Integrated Framework: Application Techniques*, AICPA, New York, N.Y., 2004, p. 28.

EXHIBIT 3: INDUSTRY PORTFOLIO OF RISKS

Source: Debra Elkins, "Managing Enterprise Risks in Global Automotive Manufacturing Operations," presentation at the University of Virginia, January 23, 2006. Permission granted for use.

Interviews and Self-Assessment

This technique combines two different processes. First, each individual of the organizational or operating units is given a template with instructions to list the key strategies and/or objectives within his or her area of responsibility and the risks that could impede the achievement of the objectives. Each unit is also asked to assess its risk management capability using practical framework categories such as those contained in the COSO ERM framework. A sample template is presented in Exhibits 4A-D. The completed documents are submitted to the ERM staff or coordinator, which could be the CFO, controller, COO, or CRO (chief risk officer). That group follows up with interviews to clarify issues. Eventually, the risks for the unit are identified and defined, and a risk management capability score can be determined from a five-point scale, as used in Exhibit 4D. Of course, organizations following the COSO 2017 ERM framework would want to adapt Exhibit 4D to match the components from that framework. Interviews might be used in conjunction with a facilitated workshop.

EXHIBIT 4A: RISK IDENTIFICATION TEMPLATE

1. Please list the major strategies and/or objectives for your area of responsibility.
2. Please list the major risks your unit faces in achieving its objectives. List no more than 10 risks.
3. Please assess the overall risk management capability within your area of responsibility to seize opportunities and manage the risks you have identified.

EXHIBIT 4B: MAJOR STRATEGIES/OBJECTIVES FOR YOUR UNIT

Please list the major strategies/objectives for your unit.

EXHIBIT 4C: MAJOR RISKS FOR YOUR UNIT

Please list the major risks your unit faces in achieving your objectives. List no more than 10 risks.

EXHIBIT 4D: RISK MANAGEMENT CAPABILITY

Use the following categories* to assess the overall risk management capability within your area of responsibility to seize opportunities and manage risks using the scale at the bottom of the page.

Internal Environment	VL	L	M	H	VH
Objective Setting	VL	L	M	H	VH
Event Identification	VL	L	M	H	VH
Risk Assessment	VL	L	M	H	VH
Risk Response	VL	L	M	H	VH
Control Activities	VL	L	M	H	VH
Information/communication	VL	L	M	H	VH
Monitoring	VL	L	M	H	VH

What is your level of concern with respect to the overall risk management capability of your area of responsibility to seize opportunities and manage risks? Please circle the most appropriate response:

VL = Very Low L = Low M = Medium H = High VH = Very High

*The categories are taken from COSO, *Enterprise Risk Management—Integrated Framework: Executive Summary*, AICPA, New York, N.Y., 2004.

Facilitated Workshops

After the information is completed and collected, a cross-functional management team from the unit or several units might participate in a facilitated workshop to discuss it. Again, using voting software, the various risks can be ranked to arrive at a consensus of the top five to 10, for example. As noted previously, using interactive voting software allows the individuals to identify and rank the risks anonymously without fear of reprisal should their superior be a member of the group.

Workshops can also be used to review environment scans and changes from a variety of sources (political, economic, technology, and so forth) to identify potential risks. Others use futures-type workshops in which a futurist takes the traditional environmental scan found in a planning process and "forces" the internal team of experts to take it longer, deeper, and wider, thereby increasing the possible range of risks identified. Other organizations have found success in black swan and strategic disruption workshops. In these workshops, the business model and related assumptions are challenged to ensure all strategic risks are identified and fully understood. An extension of this workshop is to include customers, suppliers, or other stakeholders in an attempt to develop deeper insights.

SWOT Analysis

SWOT (strengths-weaknesses-opportunities-threats) analysis is a technique often used in the formulation of strategy. The strengths and weaknesses are internal to the company and include the company's culture, structure, and financial and human resources. The major strengths of the company combine to form the core competencies that provide the basis for the company to achieve a competitive advantage. The opportunities and threats consist of variables outside the company and typically are not under the control of senior management in the short run, such as the broad spectrum of political, societal, environmental, and industry risks.

For SWOT analysis to be effective in risk identification, the appropriate time and effort must be spent on thinking seriously about the organization's weaknesses and threats. The tendency is to devote more time to strengths and opportunities and give the discussion of weaknesses and threats short shrift. Taking the latter discussion further and developing a risk map based on consensus will ensure that this side of the discussion gets a robust analysis. In a possible acquisition or merger consideration, a company familiar to the authors uses a SWOT analysis that includes explicit identification of risks. The written business case presented to the board for the proposed acquisition includes a discussion of the top risks together with a risk map.

Risk Questionnaires and Risk Surveys

A risk questionnaire that includes a series of questions on both internal and external events can also be used effectively to identify risks. For the external area, questions might be directed at political and social risk, reputation risks, regulatory risks, industry risk, economic risk, environmental risk, competition risk, and so forth. Questions on the internal perspective might address risks relating to customers, creditors/investors, suppliers, operations, products, production processes, facilities, information systems, and so on. Questionnaires are valuable because they can help a company think through its own risks by providing a list of questions around certain risks. The disadvantage of questionnaires is that they usually are not linked to strategy.

Rather than a lengthy questionnaire, a risk survey can be used. In one company, surveys were sent to both lower- and senior-level management. The survey for lower management asked respondents to "List the five most important risks to achieving your unit's goals/objectives." The survey to senior management asked participants to "List the five most important risks to achieving the company's strategic objectives." The survey instruments included a column for respondents to rank the effectiveness of management for each of the five risks listed, using a range of 1 (ineffective) to 10 (highly effective). Whether using a questionnaire or survey, the consolidated information can be used in conjunction with a facilitated workshop. In that session, the risks are discussed and defined further.

Scenario Analysis

Scenario analysis is a particularly useful technique in identifying strategic risks where the situation is less defined and "what-if" questions should be explored. Essentially, this technique is one way to uncover risks where the event is high impact/low probability.[6] In this process,

> "Managers invent and then consider, in depth, several varied stories of equally plausible futures. The stories are carefully researched, full of relevant detail, oriented toward real-life decisions, and designed (one hopes) to bring forward surprises and unexpected leaps of understanding."[7]

Using this technique, a cross-functional team could consider the long-term effects resulting from a loss of reputation or customers or from the lack of capability to meet demand. Another relevant question to ask is, "What paradigm shifts in the industry could occur, and how would they impact the business?"

The risk management group of one company uses scenario analysis to identify some of its major business risks.[8] One risk for this company is an earthquake. Its campus of more than 50 buildings is located in the area of a geological fault. From a holistic perspective, the loss from an earthquake is not so much the loss of the buildings but the business interruption in the product development cycle and the inability to serve customers. The company's risk management group analyzed this disaster scenario with its outside advisors and attempted to quantify the real cost of such a disaster, taking into account how risks are correlated. In the process, the group identified many risks in addition to property damage, including:

- "Director and officer liability if some people think management was not properly prepared,
- Key personnel risk,
- Capital market risk because of the firm's inability to trade,
- Worker compensation or employee benefit risk,
- Supplier risks for those in the area of the earthquake,
- Risk related to loss of market share because the business is interrupted,
- Research and development risks because those activities are interrupted and product delays occur, and
- Product support risks because the company cannot respond to customer inquiries."[9]

This example reveals the value of using scenario analysis: A number of risks are potentially present within a single event, and the total impact could be very large. Another scenario that this company's risk management group analyzed was a stock market downturn (or bear market). The group also defined five or six other scenarios. Under each one, it identified as many material risks as could be related to the scenario and developed white papers on each one for executive management and the board.[10]

---

[6] Deloitte & Touche LLP, *The Risk Intelligent Enterprise: ERM Done Right*, Deloitte Development LLC, 2006, p. 4.
[7] Peter Schwartz, *The Art of the Long View*, Currency Doubleday, New York, N.Y., 1991, p. xiii.
[8] Thomas L. Barton, William G. Shenkir, and Paul L. Walker, *Making Enterprise Risk Management Pay Off*, Financial Executives Research Foundation, Upper Saddle River, N.J., 2001, pp. 132-135.
[9] *Ibid.*, p. 133.
[10] *Ibid.*, p. 135.

Using Technology

The risk identification process can also utilize the company's existing technology infrastructure. For example, most organizations utilize an intranet in their management processes. The group responsible for a company's ERM process can encourage units to place their best risk practices on the ERM site. Risk checklists, anecdotes, and best practices on the intranet serve as stimulation and motivation for operating management to think seriously about risks in its unit. Also, tools that have been found particularly useful to various units can be catalogued. As new projects are launched, business managers are encouraged to consult the risk management group's intranet site.

Another use of technology is to recognize the company's potential risk that resides with the internet. For example, a company's products, services, and overall reputation are vulnerable to internet-based new media like blogs, message boards, emailing lists, chat rooms, and independent news websites. Some companies devote information technology resources to scan the blogosphere continuously for risks related to the company's products, services, and reputation.

Other companies combine technology and data (both structured and unstructured) with tools such as scenario analysis workshops, and a few use artificial intelligence (AI). One company uses AI to review unstructured data by country with an end product of patterns that are to be used in the scenarios. Another company combines data trends with the scenarios so it can see when strategy is too far off course, potentially leading to course corrections before it's too late.

Other Techniques

Many organizations calibrate their set of identified risks by comparing their risks to external sources of risks. For example, the World Economic Forum generates a set of top risks each year. Another method for calibrating is to benchmark with a peer organization and compare what each has identified. One final method for benchmarking the identified risks is to review the Item 1a risk factors (which is a required U.S. Securities & Exchange Commission, or SEC, disclosure) of other companies to see if any risks are mentioned that your organization has not considered.

Some organizations have separate risk identification techniques for identifying emerging risks. COSO's 2017 ERM framework notes that emerging risks appear after business contexts change. Principle 15 of that framework says that organizations need to identify and assess changes (potentially from the internal or the external environment). A 2017 ERM Summit at St. John's University Center for Excellence in ERM focused on emerging risks. Companies participating in the summit identified sources of emerging risks including operational incidents, industry reports, where start-ups are investing, customer satisfaction surveys, macroeconomic news, industry conferences, client input, and value shifts in the market.

Another new technique for risk identification includes strategic risk analysis. COSO's 2017 ERM framework notes that strategic risks can derive from a company misaligned with its strategy, from the chosen strategy and from the risks to implementing the strategy. This perspective, along with a lot of big changes in data, business models, innovation, disruption, and so forth has led to a new emphasis on strategic risk identification. The IMA SMA titled "Strategic

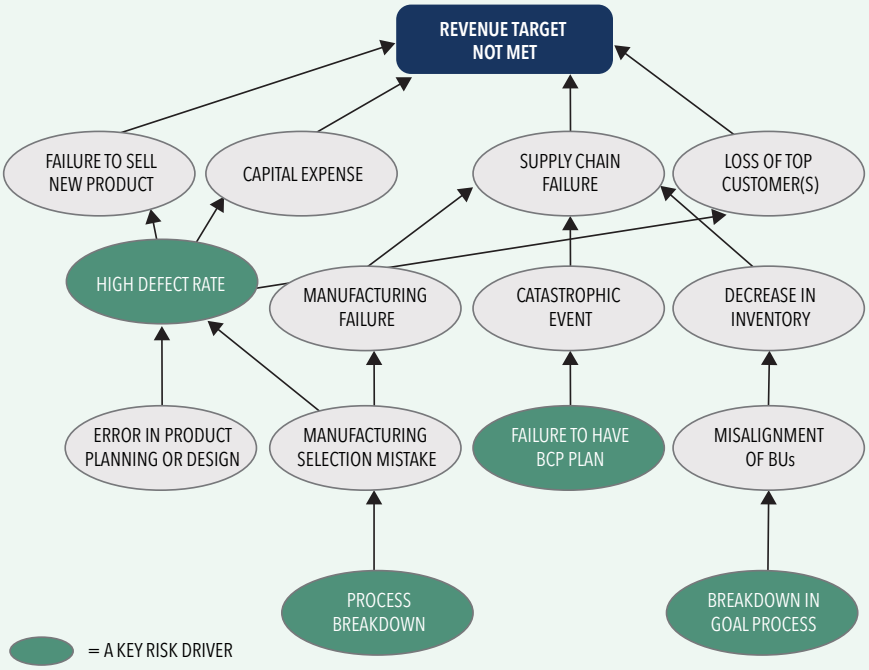
Risk Management: Optimizing the Risk-Return Profile" is a good starting point for strategic risk identification in addition to reviewing the COSO 2017 ERM framework.[11] Tools in this area are growing, but some traditional tools such as business model analysis and value chain analysis can be useful for identifying strategic risk. Other companies are trying to use black swan workshops and strategic disruption workshops to pull out the strategic risks facing their business model.

V. Analysis of Risk By Drivers

After a risk is identified, the temptation to quantify it before further analysis is completed should be avoided. Additional understanding of the risk's potential causes is required by the ERM team and management before its impact can be quantified. Working with the various units of the organization that own parts of the risk, the ERM team should drill into the risk to uncover what is beneath the surface and to get a better understanding of the potential risk drivers. An influence diagram or root cause analysis can be developed using scenario analysis. This can be done by using supporting documentation and interviewing those who own parts of the risk. Exhibit 5 presents an influence diagram for a strategic risk provided by a senior manager of ERM at a major company. In this exhibit, a chain of likely events within a given scenario is spelled out where a strategic risk—revenue target not met—has been identified.

EXHIBIT 5: INFLUENCE DIAGRAM

Develop Influence Diagram and Quantify the Risk Drivers: Define root causes and main drivers of the risks. Define the chain of events in likely scenario. Drivers should be small enough in scope that they can be quantified.



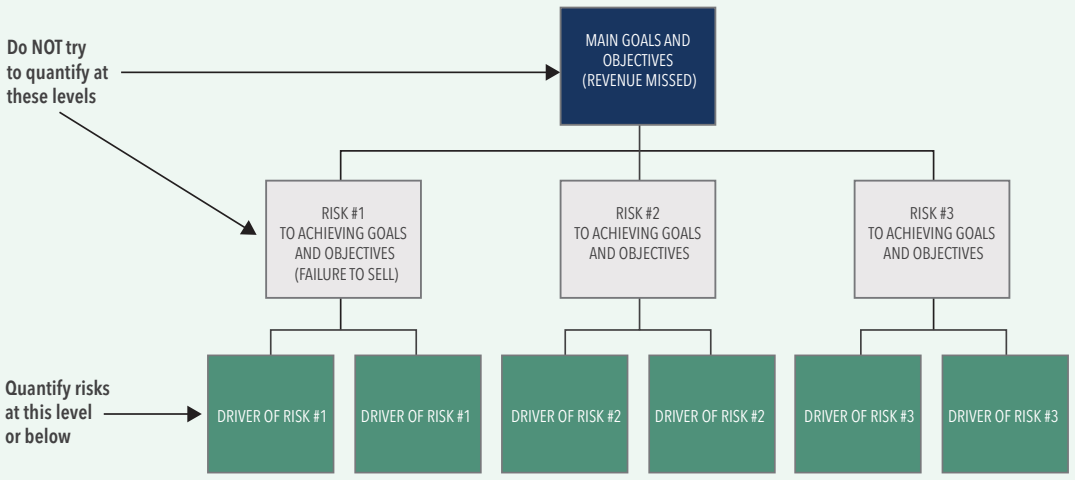
[11] James Lam, "Strategic Risk Management: Optimizing the Risk-Return Profile," IMA, 2016, www.imanet.org/insights-and-trends/risk--management/strategic-risk-management?ssopc=1.

Studying Exhibit 5, the inquiry to determine the likely drivers in a scenario for the risk of not meeting the revenue target could be the following:

- Failure to sell a new product;
- The new machinery and equipment purchased for making the new product was not selected properly because of a process breakdown in the acquisition. This led to manufacturing failures attributed to product design problems, which led to a high rate of product defect;
- Failure in the supply chain impacted the ability to meet the revenue target. A catastrophic event occurred at a major supplier, and the business continuity plan recognized this event too late to find alternative suppliers;
- Together, the above events would result in losing some top customers because high-quality products could not be delivered when required. Furthermore, in digging deeper, some misalignment of specific goals might exist in the silos involved. For example, manufacturing might have a goal of cutting cost; customer service naturally will want low defects in the products; the pricing function will be seeking high margins for the products; and the sales force is motivated to generate revenue.

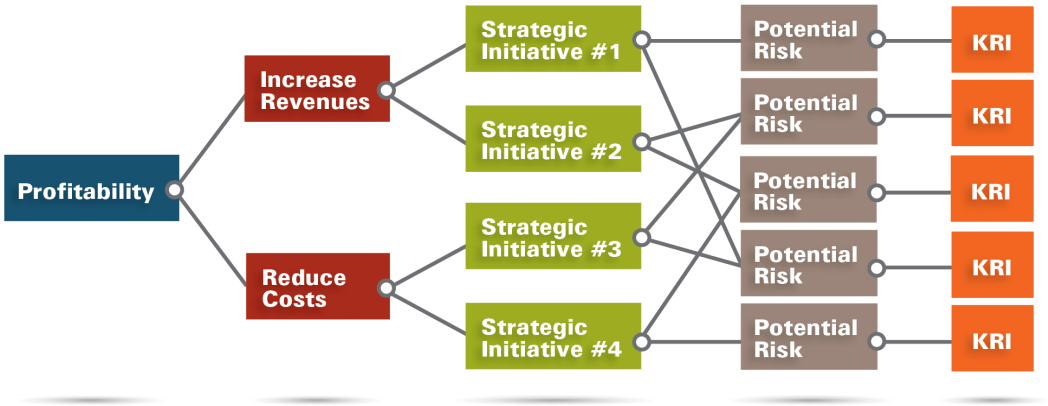
With an in-depth understanding of how the strategic risk could occur, more information is now available to assist in quantifying the risk. This information can be framed as noted in Exhibit 6 in order to begin estimating the impact. The point of this analysis is to understand the level at which quantification can best occur. If the risk is quantified at too high a level, it could end to be too broad or not actionable. Using a building block approach around risk drivers facilitates the quantification process. At the end of the process, however, quantification is still an estimate and should be viewed as merely providing an "order of magnitude" of the impact.

EXHIBIT 6: QUANTIFYING RISK—DETERMINE THE DRIVERS



Similar to analyzing risk by drivers is COSO's "Developing Key Risk Indicators to Strengthen Enterprise Risk Management."[12] Key risk indicators (KRIs) are helpful in being early indicators of change in a risk. KRIs can be linked to risk, strategies, and profits, as seen in Exhibit 7.

EXHIBIT 7: LINKING OBJECTIVES TO STRATEGIES TO RISKS TO KRIs



VI. Risk Assessment Tools

Risks must be identified correctly before an organization can take the next step. Assessing the wrong list of risks or an incomplete list of risks is futile. Organizations should make every possible effort to ensure they have identified their risks correctly using some or all of the approaches discussed. The act of identifying risks is itself a step on the risk assessment road. Any risks identified, almost by default, have some probability of influencing the organization.

Categories

Once risks are identified, some organizations find it helpful to categorize them. This may be a necessity if the risk identification process produces hundreds of risks, which can be overwhelming and seem unmanageable. Risk categories include hazard, operational, financial, and strategic. Other categories are controllable or noncontrollable and external or internal. Categorizing risk requires an internal risk language or vocabulary that is common or unique to the organization in total, not just to a particular subunit or silo. Studies have shown that an inconsistent language defining risks across an organization is an impediment to an effective ERM strategy. Risk terms would certainly vary between a pharmaceutical company and a technology company or between a nonprofit and an energy company. Several risks could be grouped around a broader risk, such as reputation risk. Other methods for categorizing risk can be financial or nonfinancial and insurable or noninsurable. Some companies also categorize risks as quantifiable or nonquantifiable.

[12] Mark S. Beasley, Bruce B. Branson, and Bonnie V. Hancock, "Developing Key Risk Indicators to Strengthen Enterprise Risk Management," COSO, 2010.

Knowing the risk categories is sometimes a step toward understanding risk interconnectedness. COSO's 2017 ERM framework emphasizes the importance of taking a portfolio view. In fact, Principle 14 is about developing a portfolio view. Although few companies do correlation matrices, one method of a portfolio view can be seen in Exhibit 8. Knowing risk interdependencies can help an organization manage risk better and see if the total risk profile aligns with risk appetite.

EXHIBIT 8: PORTFOLIO VIEW OF RISK

Qualitative vs. Quantitative

As Exhibit 9 shows, risk assessment techniques can vary from qualitative to quantitative. The qualitative techniques can be a simple list of all risks, risk rankings, or risk maps. A list of risks is a good starting point. Even though no quantitative analysis or formal assessment has been applied to the initial list of risks, the list and accompanying knowledge is valuable. Some risks on the list may not be quantifiable. For these risks, identifying them and adding them to a priority list may be the only quantification possible. Organizations should not be concerned that they cannot apply sophisticated modeling to every risk.

EXHIBIT 9: QUALITATIVE AND QUANTITATIVE APPROACHES TO RISK ASSESSMENT

QUALITATIVE:	QUALITATIVE/QUANTITATIVE:	QUANTITATIVE:
Risk identification	Validation of risk impact	Probabilistic techniques:
Risk rankings	Validation of risk likelihood	Cash flow at risk
Risk maps	Validation of correlations	Earnings at risk
Risk maps with impact and likelihood	Risk-corrected revenues	Earnings distributions
Risks mapped to objectives or divisions	Gain/loss curves	EPS distributions
Identification of risk correlations	Tornado charts	
	Scenario analysis	
	Benchmarking	
	Net present value	
	Traditional measures	

Level of difficulty and amount of data required

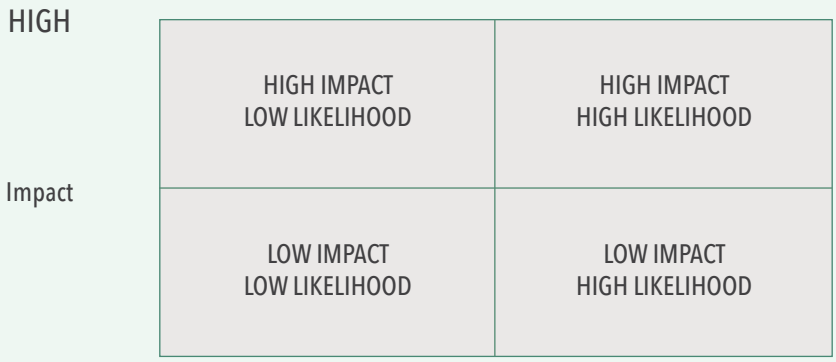
Risk Rankings

Once an organization has created its list of risks, it can begin to rank them. Ranking requires the ERM team to prioritize the risks on a scale of importance, such as low, moderate, and high. Although this seems unsophisticated, the results can be dramatic. Organizations find considerable value in having conversations about the importance of a risk. The conversations usually lead to questions about why one group believes the risk is important and why others disagree. Again, this process should use a cross-functional risk team so that perspectives from people across the entire organization are factored into the rankings. This is a critical task requiring open debate, candid discussion, and data (for example, tracking, recording, and analysis of historical error rates on a business process) where possible.

Impact and Probability

The importance of an event considers not just its impact but also its likelihood of occurring. Therefore, many ERM organizations generate risk maps using impact and probability. In ERM implementation, companies not only generate risk maps to capture impact and likelihood but also to demonstrate how risks look when put together in one place. The value of the map is that it reflects the collective wisdom of the parties involved. Furthermore, risk maps capture considerable risk information in one place that is easily reviewed. A basic risk map, such as in Exhibit 10, captures both impact and likelihood.

EXHIBIT 10: RISK MAP



When assessing likelihood or probability, the ERM team can use a variety of scales:

- Low, medium, or high;
- Improbable, possible, probably, or near certainty; and
- Slight, not likely, likely, highly likely, expected.

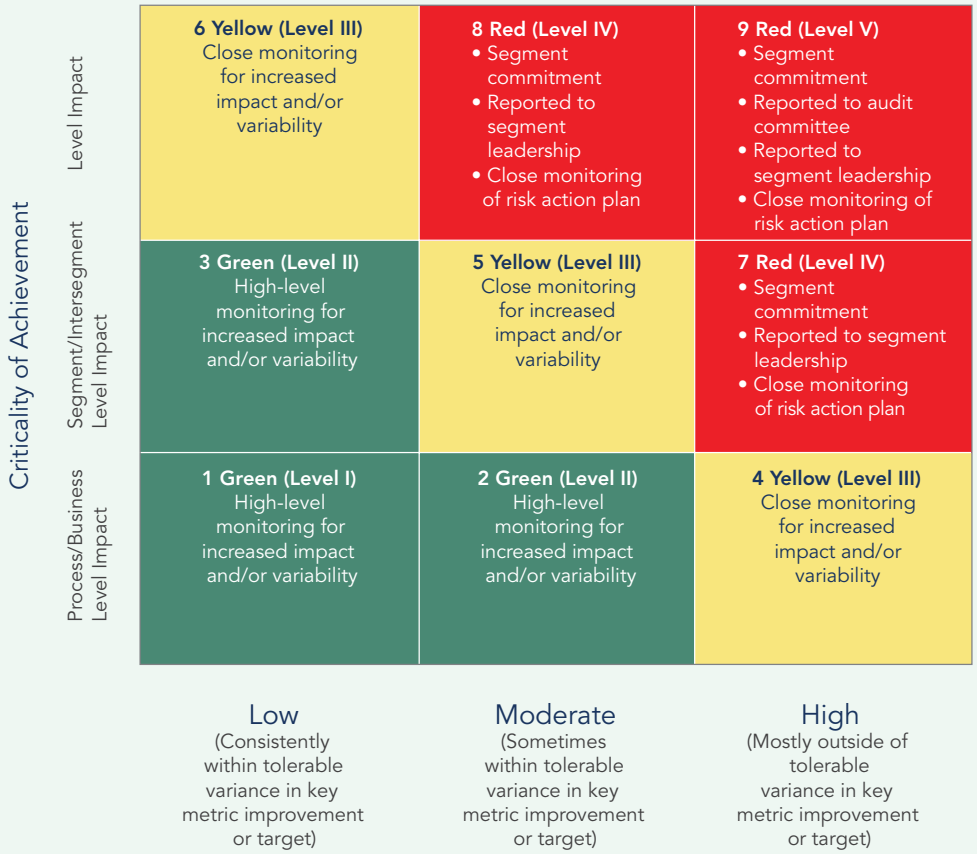
The same is true for assessing impact:

- Low, medium, or high impact;
- Minor, moderate, critical, or survival; and
- Dollar levels, such as $1 million, $5 million, and so forth.

When qualitatively assessing these risks, it is also possible to estimate ranges. For example, a company might determine that there is a low probability of a customer-related risk having an impact of $100 million, a moderate probability (or best guess) of a $50 million impact, and a high probability of a $10 million impact. Many organizations are now adding other dimensions beyond dollars to help them determine the impact of a risk, including the impact from reputation, environment, health, and so on.

Risk maps can help an organization determine how to respond to a risk. As organizations see the greater risks, they can plan a response. For example, one risk map approach used by a company is shown in Exhibit 11. For risks that are in the lower levels of impact and probability—the green zone on the map—a company should respond with high-level monitoring. For risks with higher levels of impact and probability—the red zone risks on the map—a company should take a stronger response and a higher level of commitment to managing them. Another recent addition to risk maps is adding the velocity of risks. Many leaders today want to try to understand how quickly a risk is moving. Additionally, some companies prefer to use different dimensions instead of impact and likelihood, instead choosing to plot impact and management preparedness or other dimensions.

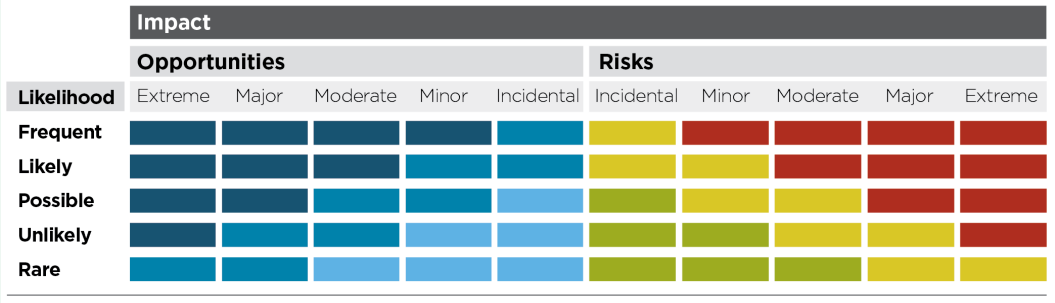
EXHIBIT 11: RISK MAP MODEL



One very positive use of a risk map can be to create risk and opportunity maps. Many business professionals have a natural tendency to think of risk in a negative way. Risk and opportunity maps can put the pressure on to seriously consider the opportunity (and the full upside) related to the perceived risk. See Exhibit 12, taken from COSO's "Risk Assessment in Practice."[13]

[13] Patchin Curtis and Mark Carey, "Risk Assessment in Practice," COSO, 2012.

EXHIBIT 12: ILLUSTRATIVE COMBINED RISK AND OPPORTUNITY MAP



Keys to Risk Maps

Several keys need to be considered when generating risk maps: confidentiality, definitions, time frame, direction, and correlations. Organizations may want to consider doing impact and probability in a confidential manner. As noted previously, software tools are available to facilitate confidential sharing. On the other hand, some companies find that openly sharing assessments within the group is acceptable. Even with confidentiality, good risk facilitators can bring out the risk source and root problems.

Definitions used during the risk map generation are critical. What is "important" to one work unit or individual may not seem "important" to another. If organizations measure impact in dollars, the dollars must be without ambiguity. Does the risk influence dollars on one product, dollars for a certain division, or earnings per share? Similarly, "improbable" might be interpreted by some to be 1% while others could think it means 15%. These definitions and terms should be clearly established before the risk map sessions are conducted.

Closely related to definitions are time frames, which need to be established up front so that any understanding of the risk and its impact is clear as to when it will affect the organization. An assessment of risk at one point in time has the same failings as strategic plans and objectives, which do not take a longer-term perspective on market trends, customer needs, competitors, and so on. What seems important today or this week may not seem important in five years. Similarly, although some longer-range risks may not seem important today, these risks could threaten the organization's survival if left unmanaged.

Some organizations find it valuable to capture the direction of the risk. This can be labeled on the risk map or communicated separately. Direction of risk can be captured using terms such as "increasing," "stable," or "decreasing." Related to the risk direction is the risk trend. Knowing the direction and trend of a risk as well as its dollar impact and likelihood can be crucial to managing that risk. For example, risk trends can reveal that the risk was decreasing over the last several years but has increased recently.

One weakness in risk maps (and in silo risk management) is that maps do not capture any risk correlations. Ignoring risk correlations can lead to ineffective and inefficient risk management. Risk correlations can be considered for financial risks or nonfinancial risks. Clearly,

how some companies manage one foreign currency exposure should be considered with how they manage another foreign currency exposure. Managing these in silos (without an enterprise-wide approach) can be inefficient because dollar exposures to only the yen or euro ignore that the yen and euro are correlated. Similarly, silo risk management would ignore the fact that the movement of interest rates could influence an organization's pension obligations and debt obligations differently. As another example, how an organization manages commodity exposure today should be factored in with how it plans to change its long-term strategy to manage that same exposure. Short-term solutions of foreign currency risk management are different from long-term solutions of building plants in other countries. As is evident, correlations among risks and an enterprise-wide approach are critical.

Link to Objectives at Risk or Divisions at Risk

Identifying risks by objective gives an organization the option to map risks by objectives. For nonprofit organizations, this may be more important because earnings per share is not the biggest concern. A risk map by objective captures all the risks related to a single objective, helping the organization understand the broad spectrum of risks facing that objective. For example, the objective of maintaining the corporate reputation at a certain level could have many risks to be mapped. Using such a map, the organization can see the biggest risks to reputation. Similarly, risks can also be identified by division, which may be more informative for division managers. Organizations can generate risk maps for each division and for the organization overall.

Residual Risk

After organizations assess risks, they should also consider any related controls so that the residual risk is known. A residual risk is the remaining risk after mitigation efforts and controls are in place to address the initially identified inherent risks that threaten the achievement of objectives. Risk maps can show overall risks, or they can be shown with just residual risks. Understanding residual risk can provide major benefits because companies do not want to over- or under-manage a risk that may be deemed by management and stakeholders to be "tolerable" or acceptable relative to stated business objectives. This is a major reason why some companies adopt ERM and try to understand, even qualitatively, the return on investment (ROI) of an ERM program. In the process of identifying risks and controls, the management team/process owners clearly play a leadership role, but there is a system of "checks and balances" in the control environment. For example, the control environment for internal controls over financial reporting includes the audit committee as well as internal and external auditors.

Validating the Impact and Probability

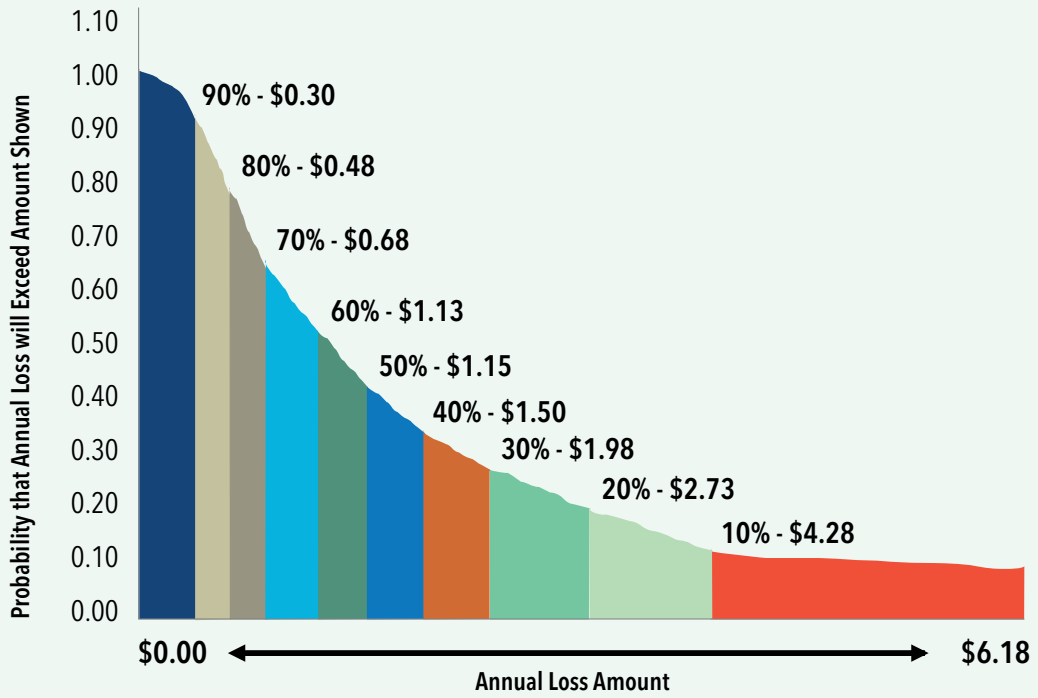
Organizations can validate the qualitative assessments of initial impact and probability by examining historical data to determine the frequency of events or the impact such events have had in the past. Events that have happened to other organizations can be used to understand

how a similar event might impact your own organization. Gathering such data can be time-consuming, but it has certain advantages. Knowing the real frequency or likelihood of a major drop in sales, for example, can provide an organization with the information necessary to make informed cost-benefit decisions about potential solutions.

Gain/Loss Curves

Gain/loss curves are useful tools because they help an organization see how a risk can influence its financial statements and result in a gain or a loss. Furthermore, gain/loss curves also reveal the distribution of potential gains and losses. Gain/loss curves do not show correlations between risks, however, and they do not show all the risks in one place. A gain/loss curve is presented in Exhibit 13. The curve shows how much money the company loses or gains from a specific risk. The horizontal axis represents dollars, and the vertical axis represents probability. The sample curve in Exhibit 13 shows that the organization loses $1.15 million on average (at 50% probability in this illustration) as a result of this risk. Moving along the probability scale shows that, 90% of the time, this organization loses $300,000 because of this risk. The organization believes it loses $4.28 million about 10% of the time. Knowing how big of an impact a risk causes over a distribution of probabilities provides management with the information necessary to decide how much money to spend managing the risk. Gain/loss curves can also reveal that some risks occasionally generate gains instead of losses. Developing gain/loss curves can require substantial data collection, and a company has to balance the data collection efforts with the benefits obtained.

EXHIBIT 13: GAIN/LOSS PROBABILITY CURVE

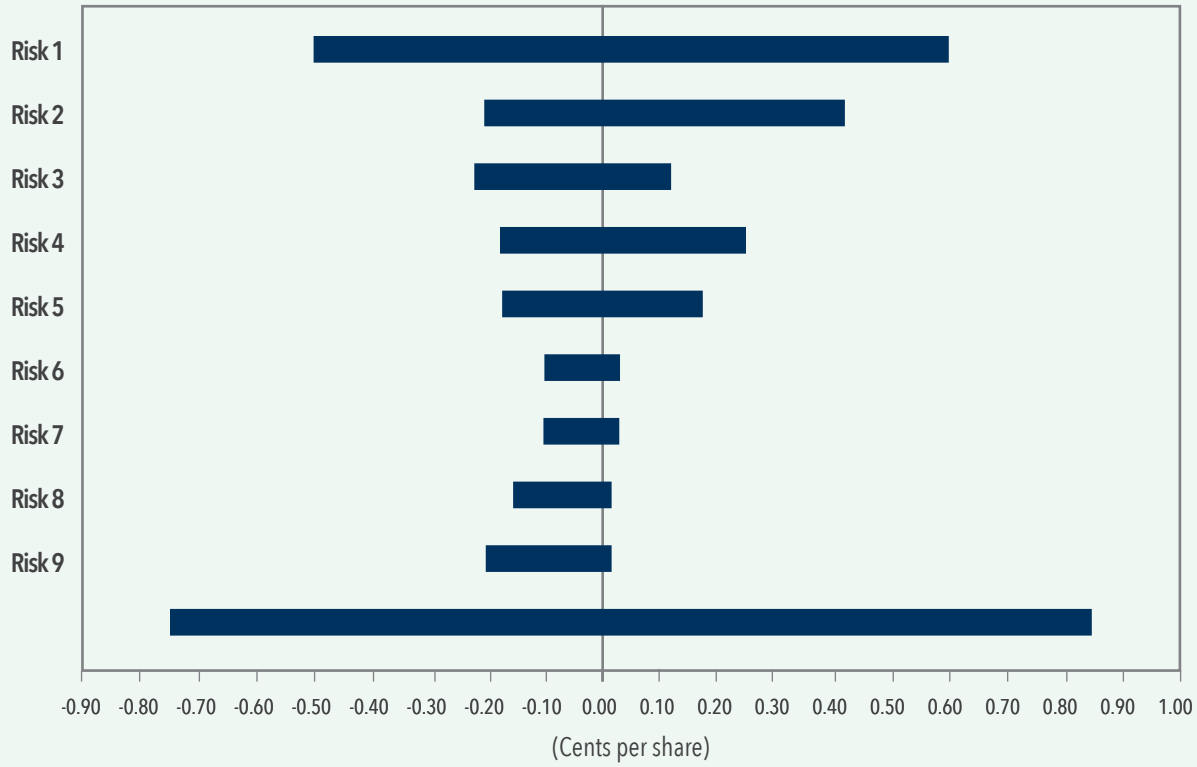


Note: All loss amounts are in millions of dollars.

Tornado Charts

Similar to gain/loss curves, tornado charts attempt to capture how much of an impact a risk has on a particular metric such as revenue, net income, or earnings per share. Exhibit 14 shows an example of a tornado chart. Tornado charts do not show correlations or distributions, but they are valuable because executives can see, in one place, the biggest risks in terms of a single performance metric.

EXHIBIT 14: TORNADO CHART—EARNINGS VARIABILITY BY SAMPLE RISKS



Risk-Adjusted Revenues

Risk-adjusted (or risk-corrected) revenues allow management to see how revenues could look if risks were managed better. As Exhibit 15 shows, risk-corrected revenues are smoother and more controllable. On a broader scale, Exhibit 16 shows one company's view of how better risk management affects the distribution of earnings. A tighter distribution of earnings could potentially lead to improved performance of its stock price. The two types of analysis shown in Exhibits 15 and 16 are why some companies want to implement ERM. While stakeholders (such as investors) appreciate growth in earnings, they also appreciate some level of stability and predictability and are often willing to pay a premium for these attributes. Other organizations are beginning to use risk-adjusted return on capital (risk-adjusted return/economic capital) to compare risk returns of different decisions.

EXHIBIT 15: ACTUAL REVENUE VS. RISK-CORRECTED REVENUE

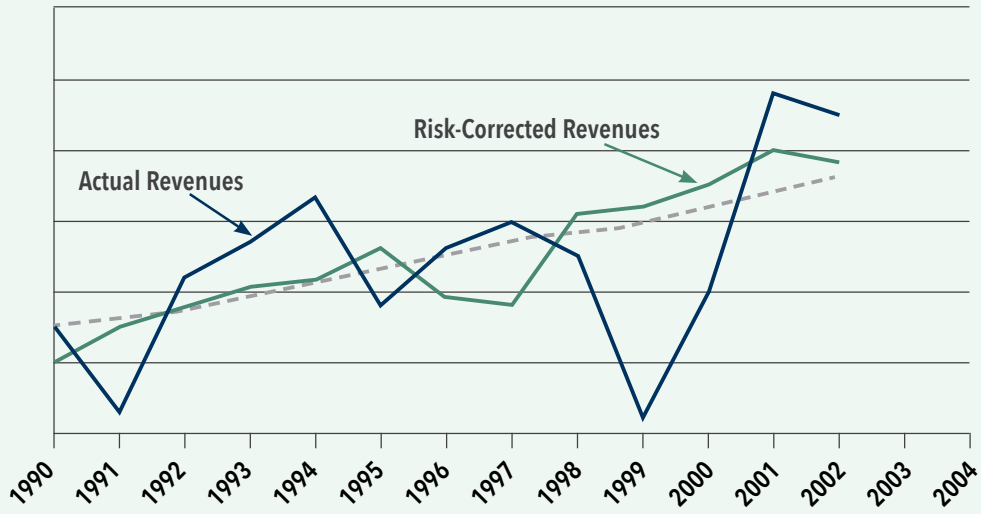
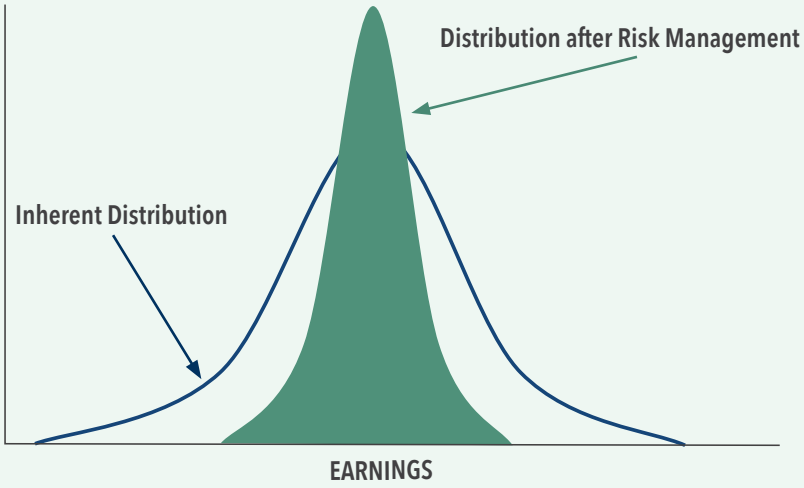


EXHIBIT 16: GOALS OF RISK MANAGEMENT



A Common Sense Approach to Risk Assessment

While some of these risk metrics and tools may seem difficult, a simple approach can yield equally good results. One approach is to measure where the company stands today on a risk issue. After implementing risk mitigation techniques, the company can reassess the risk issue. Of course, not all of the improvement related to a risk can be traced to the risk mitigation techniques, but improvement is still valuable. One major retailer uses this approach to gauge the value added from its ERM efforts in addition to other value-added metrics. This retailer identified inventory in-stock rates as a risk. Measuring in-stock rates over time gave the company a good feel for the historical levels of in-stock rates. Next, after implementing risk mitigation efforts, current inventory in-stock rates were captured. Improvements in in-stock rates are traced to improvements in sales and, ultimately, to value added from the ERM process.

Probabilistic Models

Some organizations use quantitative approaches in ERM that are built on traditional statistical and probabilistic models and techniques. The disadvantage to these approaches is that they require more time, data, and analysis and are built on assumptions. Furthermore, using the past to predict the future has limitations even before other "explanatory" variables are included in the statistical prediction process. But some organizations still find these models very useful as a tool in their solutions toolkit when approaching risk.

One technique focuses on earnings at risk, which are determined by examining how earnings vary around expected earnings. In this approach, variables are examined to see how they influence earnings, such as determining the influence that a one-point movement in interest rates would have on earnings. Similarly, expected or budgeted cash flows can be determined and then tested for sensitivity to certain risks, yielding a cash-flow-at-risk number. As Exhibit 17 shows, some companies trace the earnings at risk to individual risk sources. Knowing the actual root cause or source of the risk helps to manage it more efficiently. Companies can also trace the earnings at risk to business units to help gauge the hedge effectiveness of each business unit (see Exhibit 18). Knowing which business units have the greatest risk is valuable information. With this knowledge, a company could compare a business unit's earnings level to the earnings at risk. Those units that generate low earnings and high levels of risk may not be desirable business units. Having earnings at risk in the aggregate allows an organization to see which months have the greatest risk (see Exhibit 19). Also, distributions can be created that estimate the probability of meeting earnings targets (see Exhibit 20).

EXHIBIT 17: EARNINGS AT RISK BY RISK FACTOR

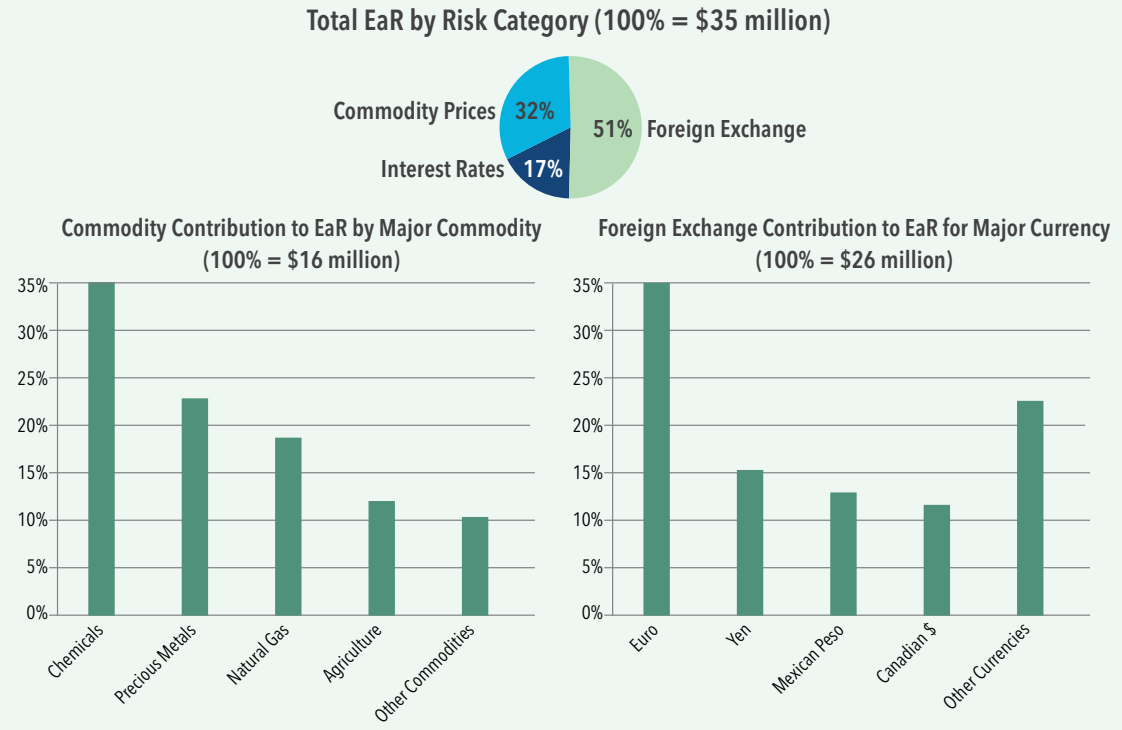


EXHIBIT 18: EARNINGS AT RISK HEDGE EFFECTIVENESS COMPARISONS

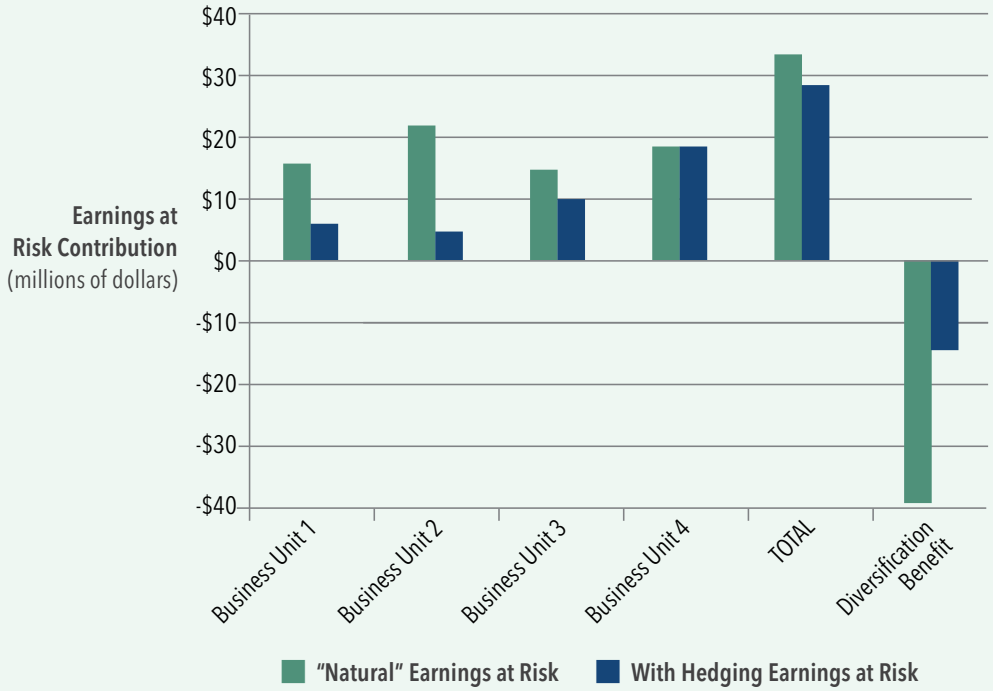


EXHIBIT 19: EXPECTED EARNINGS AND EaR

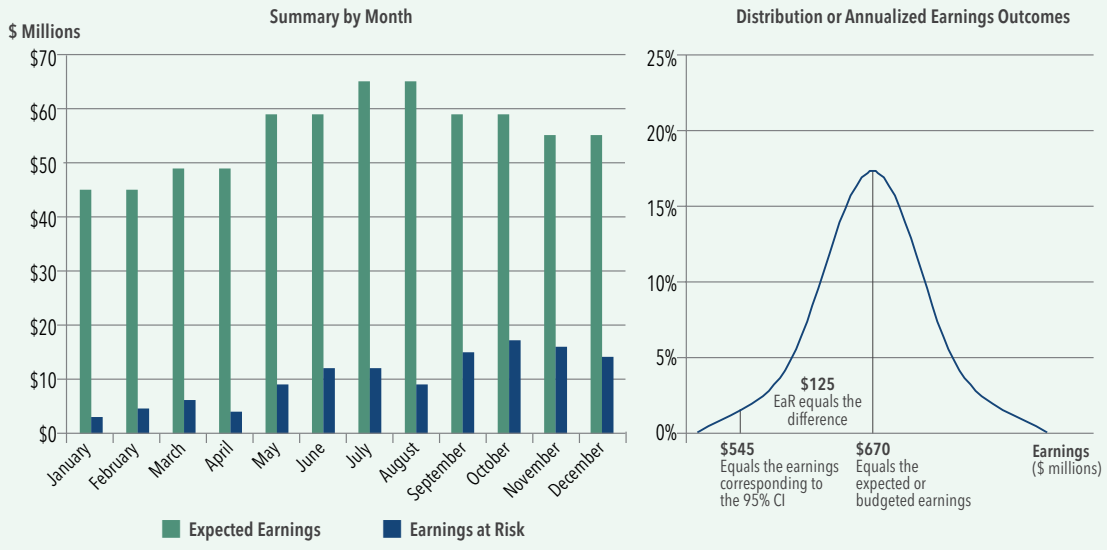
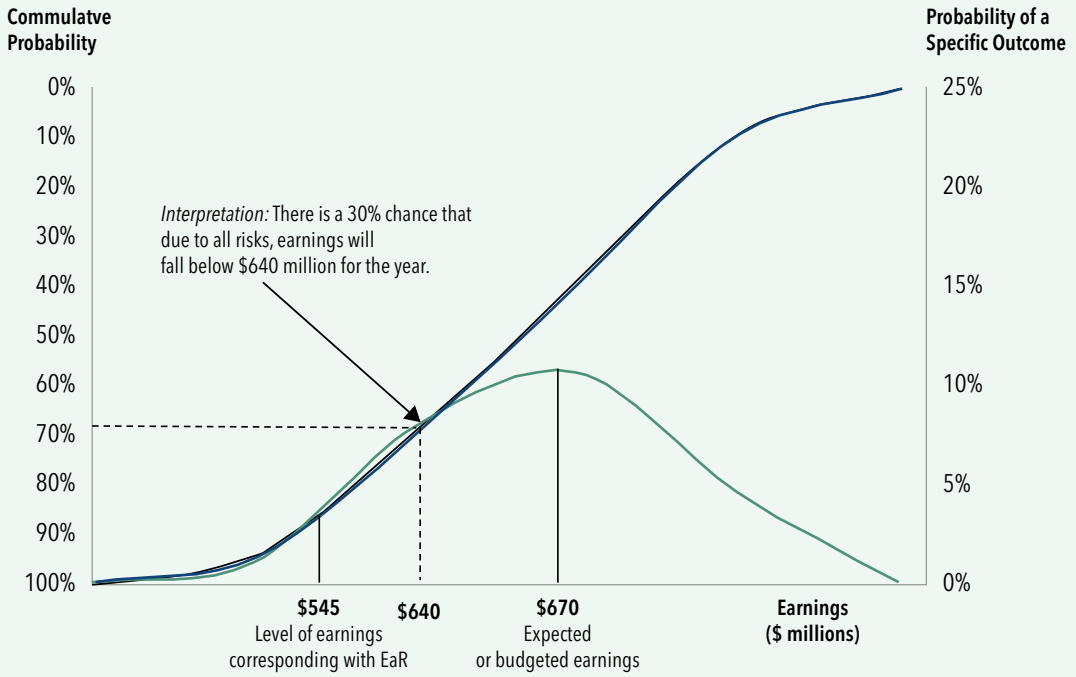


EXHIBIT 20: PROBABILITY ASSESSMENT OF EARNINGS OUTCOME



Seemingly Nonquantifiable Risks

Some risks seem to defy acceptable quantification, but a deeper look can reveal valuable information. Reputation is a risk that has become increasingly important in today's business environment, and it must be managed. At first glance, some executives would say you cannot quantify it, but it can be in some ways. In academia, for example, a university's reputation is a prodigious risk. Tracking a drop in contributions after a scandal can provide preliminary data that could lead to the ability to quantify reputation risk. Ranges of decreases in contributions could also be developed, with the maximum risk being a major decrease in donations. Gathering data from universities or other nonprofit organizations that have experienced a drop in contributions can provide valuable external data that could assist in quantifying this risk. For public companies, the impact of reputation risk could be examined by studying decreases in stock prices surrounding an event that damaged an organization's reputation. It is important to note that while this might capture and provide a quantifiable risk, it still partially ignores the damage that reputation events have on supplier or vendor relations. It also ignores how future customers might be influenced by the reputation event. Although these related risks might not be quantifiable, they highlight the importance of having an ERM team study and analyze risks very closely so that conversations about the risks are focused on managing the risk and not just on identification and measurement.

Another example of a risk that appears nonquantifiable is a breach in IT security. Examining the movement in stock price around the event, however, can help a company gather a preliminary estimate of how shareholders view the event. Additionally, talking to other

companies that have experienced IT security breaches can help the company understand the potential impact. Finally, understanding the organization's unique method of creating value for its customers can also offer critical insights regarding the impact of the breach. Companies that have customers who value trust and confidentiality, such as financial institutions, should estimate a greater impact from a potential IT security breach.

A major electronic retailer may determine that a key risk to sales is a change in gas prices. The retailer relies on consumers having discretionary income, and higher gas prices lower discretionary income and decrease the retailer's sales. The effect of gas prices on sales can be calculated and potentially planned for in advance. Another example is the risk of weather related to a snowblower company's sales. Guaranteeing a rebate to customers if the amount of snowfall is below a certain level can increase sales in years with low snowfall.[14] These examples show that while not all risks can be quantified with a sophisticated technique, valuable risk assessment and management can still be applied.

VII. Practical Implementation Considerations

The implementation of ERM depends on a number of organizational variables and no specific recipe is available to assure successful implementation in any organization. In this section, however, a number of practical considerations are discussed that may provide helpful insights in the implementation process. These include ERM infrastructure, ERM maturity models, staging ERM adoption for early wins, the role of the management accountant, ERM education and training, technology, aligning corporate culture, building a case for ERM, and the ROI of ERM.

ERM Infrastructure

Implementing ERM can take many shapes. Some organizations have only one person in charge of risk, while others employ a large team. Both approaches have advantages. With a large team, more resources and people are focused on the effort. Having a small ERM staff, however, encourages the organizational units, management, and employees to become highly involved and share responsibility for ERM. A common approach is to have a moderate number of people on the ERM team to facilitate risk workshops, help executives and business units understand their risks, gather data across the organization, and assist in reporting risks upward to senior executives and the board. Broad representation, objectivity, and a look to "the big picture" are keys. Although many approaches to ERM are found in practice, common elements include:

- CEO commitment (tone and messaging from the top),
- Risk policies and/or mission statements including adapting any company risk or audit committee charter to incorporate ERM,
- Reporting to business units, executives, and the board,
- Adoption or development of a risk framework,
- Adoption or development of a common risk language,

[14] Stephen W. Bodine, Anthony Pugliese, and Paul L. Walker, "A Road Map to Risk Management," *Journal of Accountancy,* December 2001, pp. 65-70.

- Techniques for identifying risk,
- Tools for assessing risks,
- Tools for reporting and monitoring risk,
- Incorporating risk into appropriate employees' job descriptions and responsibilities,
- Incorporating risk into the budgeting function, and
- Integrating risk identification and assessment into the strategy of the organization.

ERM Maturity Models

Once an organization has implemented ERM, an appropriate question arises about the progress being made in ERM. As a result, a number of ERM maturity models have been developed. One organization categorizes ERM development into three phases: (1) building a foundation, (2) segment-level ERM, and (3) enterprise-level ERM. Each phase is broken down into three stages, shown in Exhibit 21. Phase one involves building executive support, building the core model, aligning expectations, and developing segment-level risk management commitments. Phase two covers executing a consistent risk framework, engagement in specific areas and by segment-

EXHIBIT 21: ERM MATURITY MODEL

Phase I: Building a Foundation for Business Risk Management	Phase II: Segment-Level Business Risk Management	Phase III: Enterprise-Level Business Risk Management
Phase Objectives:		
• Build executive-level support • Strengthen core team and operating model • Align expectations through a risk management commitment process • Develop specific segment-level risk management commitments	• Execution of a consistent risk management approach across all segments • Engagement in specific areas to help the business remediate significant risk issues and fulfill their segment risk management commitment • Segment-level personnel at appropriate levels engaged in the risk management process • Demonstrating the tangible value of a disciplined risk management process within each segment	• Evolve to an enterprise risk commitment and accountability model by "connecting" the segment risk commitments to consider cross-segment risk issues and interdependencies • Enhance coordination and integration among segment business risk services (BRS) teams to help the enterprise remediate significant risk issues and fulfill the enterprise risk commitment • Deepen risk management focus on potential risk issues applicable to all business segments • Enhance coordination with other components of the enterprise risk management operating model that focus on specific areas of risk exposure
Stage Objectives:		
Stage 1: Awareness — Build risk management vision, strategy, and awareness	**Stage 4: Engagement** — Engagement in specific risk issues to help fulfill the risk management commitment	**Stage 7: Collaborate** — Enhance BRM collaboration across other segment teams to consider cross-segment risk issues and interdepen-dences
Stage 2: Capability — Build initial risk management foundation of structure, resources, and operating model	**Stage 5: Value** — Demonstrating tangible value from a disciplined risk management process	**Stage 8: Coordinate** — Enhance BRM coordination with other areas
Stage 3: Alignment — Align expectations through a risk management commitment	**Stage 6: Operationalize** — Segment-level personnel at all levels fully engaged in and operationalizing the risk management process	**Stage 9: Integrate** — BRM is fully integrated with business planning, performance management, quality, and other key management processes

level personnel, and demonstrating the tangible value of a disciplined process. Phase three includes connecting segment risks, enhancing coordination and integration, and deepening risk management focus. While described for a multibillion-dollar entity, this approach is scalable to organizations of any size.

Maturity models do more than inform a company of its progress in ERM. They can influence a company's rating from rating agencies, too. Standard & Poor's now applies an ERM maturity model to certain companies and industries, such as the insurance and banking industries as well as some energy companies. Consequently, ERM implementation could eventually impact a company's cost of capital and capital adequacy. For example, Standard & Poor's evaluates an insurer's ERM practices by considering the risk management culture, risk controls, emerging risk management, risk and capital models, and strategic risk management. These lead to an ERM score of weak, adequate, strong, or excellent.

Some believe that you can't just have ERM—you must also have effective board risk oversight to manage risks effectively. Of course, COSO's 2017 ERM framework's first component is governance and culture. Additionally, the SEC has required disclosures about board risk oversight for those subject to their regulations. As such, even board risk oversight can be assessed or benchmarked on dimensions of how it is set up and whether it works. Too many headlines from company debacles about boards not knowing risks suggests such as assessment is a worthwhile practice. IMA and the Association of Chartered Certified Accountants (ACCA) published a study called "A Risk Challenge Culture," which listed some board risk best practices.[15] Similarly, the Institute of Internal Auditors (IIA) published the research project "Improving Board Risk Oversight through Best Practices."[16] These two projects would make a great starting point for trying to assess board risk oversight practices.

Staging ERM Adoption for Early Wins

ERM implementation is a change management project in which an organization moves to risk-informed decision making. The goal is to improve the confidence of decision makers through a more explicit understanding of the risks facing the unit. ERM is a journey that takes continuous commitment from C-level executives and where implementation cannot be achieved overnight—it should proceed in incremental steps. At the same time, an organization embarking on ERM implementation needs to recognize that bad things can happen to a good project if results are not forthcoming. Consequently, striving for early wins in the ERM implementation project is important. For example, a major company (after developing its approach to ERM) chose to implement ERM in a strategic business unit that was mature and tightly controlled. In this instance, the company preferred not to roll out ERM in a unit that it knew in advance had many problems. The rollout was successful, and the unit was used as a model to help build momentum for ERM implementation in other units.

---

[15] Paul L. Walker, William G. Shenkir, and Thomas L. Barton, "A Risk Challenge Culture," IMA and ACCA, 2014, www.imanet.org/insights-and-trends/risk--management/a-risk-challenge-culture.

[16] Paul L. Walker, William G. Shenkir, and Thomas L. Barton, "Improving Board Risk Oversight through Best Practices," IIA, 2012.

In another company, the decision was to initially implement ERM with the senior-level executives. This group went through the process of identifying and assessing risks at the enterprise level and developing mitigation strategies. Once members of this group were sold on the benefits of ERM, they became ERM champions and supported its rollout to the various operating units. See Exhibit 21 for an example of staging an implementation.

The Role of the Management Accountant

As noted in the first SMA on ERM, the management accountant and finance professional can play a major role in ERM implementation by championing the process, providing expertise on the process, serving on cross-functional ERM teams, and providing thought leadership. Other key roles include assisting with the quantification of risks, analyzing the risk correlations, developing the range and distribution of a risk's impact, determining the reasonableness of likelihood estimates, benchmarking impact and likelihood against historical events and other organizations, setting and understanding risk tolerances and appetites, assessing and quantifying various alternative risk mitigation strategies, and quantifying the benefits of ERM. The management accountant of the future may be more and more accountable for risk management responsibilities. One CFO study noted four themes that enable the future success of that office: recognizing disruption, increasing the enterprise's risk IQ, thinking and communicating strategically, and developing skills to enable a forward-thinking organization.

ERM Education and Training

Some frameworks outside the United States mention the possibility of mandating ERM training. Although formal training on financial risks is more common, ERM education and training is being developed on different avenues. For example, universities such as North Carolina State and St. John's offer courses in ERM, with the latter offering both an M.S. and an MBA in ERM. Additionally, various risk management certifications are popping up around the globe from the IIA, COSO, and others. Given the management accountant's growing role in strategy management as a trusted business advisor, IMA offers a specialized credential for those with the CMA® (Certified Management Accountant) certification, the CSCA® (Certified in Strategy and Competitive Analysis). Organizations need to find their own training needs, but a list might include:

- Understanding the nature of risk—this is not as easy as it first appears if a true enterprise-wide approach is implemented,
- Understanding the legal and regulatory requirements related to risk management,
- Knowledge of ERM frameworks,
- Facilitation skills,
- Expertise in identifying risks,
- Knowledge for building risk maps,
- Reporting structures and options (what to report to the CEO, board, and audit committee),

- Software training,
- Financial risk training (options, hedging strategies, insurance options, derivatives, and so on),
- Operational risk management,
- Building and understanding control solutions,
- Developing and monitoring performance metrics related to risks,
- Change management,
- Macro risk analysis, and
- Strategic risk analysis.

Technology

Some technology tools are available to assist in the facilitation/identification phase. Additionally, software is available to assist an organization with the entire ERM process. Gartner Inc. has reviewed ERM software vendors on two aspects: completeness of vision and ability to execute.[17] Some organizations choose to either develop their own ERM processes tailored to their needs or hire consultants to help with the process. Technology products not only help with the process, but they also assist with data gathering, modeling, or reporting. One risk software tool, for example, helps with capital optimization and data management. Other technology products are designed to help with issues such as time-series modeling, correlations, and other advanced modeling techniques.

Aligning Corporate Culture

Success for many is still dependent on culture and in today's world that culture impacts how risk is managed. Many organizations will notice a change in the company culture as ERM implementation progresses. One noticeable difference is a proactive focus on risks rather than a reactive approach. Other changes are related to improved accountability and responsibility. With ERM in place, managers are more responsible for risk management and controls because they helped identify the risks and controls. As solutions and metrics are developed to better manage a risk, management can also be held more accountable for it. This increase in accountability and responsibility can flow down to lower levels in the organization. An additional change may be from a "we need to comply" perspective to "we need to manage this risk to achieve better results." Other cultural changes could occur, such as a shift from "blaming" to "identify and managing," a change in "Do not report bad news" to "Report as early as possible" (so the risk can be managed), and, finally, from a "How does this affect my area or unit?" to "How does this affect the risks of the entire organization?" Some consultants have developed cultural diagnostic tools to enable organizations to assess this cultural change. COSO's 2017 ERM framework has a principle that covers reporting on risk, culture, and performance.

[17] French Caldwell and Tom Eid, *Magic Quadrant for Finance, Governance, Risk and Compliance Management Software, 2007,* Gartner, February 1, 2007, www.gartner.com/doc/500595/magic-quadrant-fiannce-governance-risk.

The ROI of ERM

When a company has adopted ERM, the case for benefits vs. the cost and effort expended can be made by pointing to specific experiences where managing a risk added value to the bottom line. A major retailer uses metrics to track the results of its risk management initiatives. For example, the company will open many new stores in the year and must have capable store managers. From experience, the company knows that one risk is the turnover of store managers—it has historical data on turnover rates and knows the cost of recruiting and training a store manager. The human resources group adopted risk mitigation activities for the turnover risk, established targets for improvement, and monitored the results. In time, it was able to show that managing this risk reduced costs and, thus, improved the company's bottom line. The leadership of the human resources group could report to the CEO that it had indeed created shareholder value by managing this risk. In many cases, it does not take rocket science to select appropriate metrics to monitor the effectiveness of risk mitigation initiatives, and, in turn, the impact on the bottom line. While it would be desirable to calculate a ROI for the ERM effort, such a measurement would be based on many assumptions. Focusing on the benefits of managing a specific risk may offer the most persuasive evidence of how ERM creates value for the company. One study identified that the ultimate benefit is better decision making; specifically, ERM enables companies to make better decisions.

VIII. Conclusion

This SMA on ERM, along with the earlier one published by IMA, provides guidance for the leaders of organizations to identify, assess, and manage risk while, at the same time, growing the business. Because the risks in the global economy constantly change and evolve, ERM is a never-ending journey. ERM requires strong commitment from C-level executives and an effective process tailored to each organization's unique culture. A company's implementation can benefit from the ERM knowledge that CMAs and other finance professionals can bring to the process. In their quest to "drive business performance," management accounting and finance professionals should seize the opportunity to become partners with senior management and the board in ERM implementation.

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 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 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.

Additional Resources

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

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

Thomas L. Barton, 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*, 2004.

Peter L. Bernstein, *Against the Gods–The Remarkable Story of Risk*, John Wiley & Sons, Inc., New York, N.Y., 1996.

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

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

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

COSO, *Internal Control—Integrated Framework: Executive Summary*, AICPA, New York, N.Y., 1992.

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

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

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

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

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

Economist Intelligence Unit, *Enterprise Risk Management—Implementing New Solutions*, New York, N.Y., 2001.

Debra Elkins, "Managing Enterprise Risks in Global Automotive Manufacturing Operations," presentation at the University of Virginia, January 23, 2006.

Michael S. Emen, "Corporate Governance: The View from NASDAQ," NASDAQ, New York, N.Y., 2004.

Marc J. Epstein 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*, International Federation of Accountants, New York, N.Y., 1999.

Financial Reporting Council (FRC), *The Combined Code on Corporate Governance*, 2003.

FRC, *Internal Control: Revised Guidance for Directors on the Combined Code*, 2005.

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

Stephen Gates, Jean-Louis Nicolas, and Paul L. Walker. "ERM: A Process for Enhanced Management and Improved Performance," *Management Accounting Quarterly*, Spring 2012, pp. 28-38, https://bit.ly/2Ij6Wrd.

Everett Gibbs 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 Report on Corporate Governance for South Africa*, Institute of Directors in Southern Africa, 2002.

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

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

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.

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

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

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

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

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

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

Jerry A. Miccolis, Kevin Hively, and Brian W. Merkley, *Enterprise Risk Management: Trends and Emerging Practices*, The Institute of Internal Auditors Research Foundation, Altamonte Springs, Fla., 2001.

Takehiko Nagumo, "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.

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

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

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

Lucy Nottingham, "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.

Jim Presmanes and Paul L. Walker, "Improving Strategic Risk Management Using Macro Risk Analysis," RIMS, 2016.

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

Protiviti, "Guide to Enterprise Risk Management: Frequently Asked Questions. Sarbanes-Oxley Act of 2002, H.R. 3763," 2006.

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

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

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

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

Carl Smith, "Internal Controls," *Strategic Finance*, March 2006, p. 6, http://sfmagazine.com/wp-content/uploads/sfarchive/2006/03/PERSPECTIVES-Internal-Controls.pdf.

Wendy K. Smith, "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.

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

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

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

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

Patrick J. Stroh, "Enterprise Risk Management at UnitedHealth Group," *Strategic Finance*, July 2005, pp. 27-35, http://sfmagazine.com/wp-content/uploads/sfarchive/2005/07/Enterprise-Risk-Management-at-UnitedHealth-Group.pdf.

Emily Thornton, "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. SEC, "Commission Guidance Regarding Management's Discussion and Analysis of Financial Condition and Results of Operations," Release No. 33-8350, December 19, 2003.

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

Paul L. Walker, and Mark L. Frigo, "The CFO as Chief Risk Manager," CGMA, 2017.

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.

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

Paul L. Walker, William G. Shenkir, and 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.

Paul L. Walker, "Innovation and ERM: Partners in Managing the Waves of Disruption," IMA and ACCA, 2016, www.imanet.org/insights-and-trends/operations-process-management-and-innovation/innovation-and-erm-partners-in-managing-waves-of-disruption.

Paul L. Walker, *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.

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