Larry Baker brings a world of experience and a wealth of knowledge to the critical subject of enterprise risk management. In his inimitable storytelling fashion, Larry does exactly what he promises to do: Get to the truth. Larry’s book should be on the required reading list of all in the profession who seek to add value to their organizations by managing risks in an increasingly complex environment.

—Richard F. Chambers, CIA, QIAL, CGAP, CCSA, CRMA

President and Chief Executive Officer

The Institute of Internal Auditors

Lake Mary, FL

Larry Baker is one of the pioneers of ERM as he has been involved in helping organizations strengthen their risk oversight long before many of us had ever heard the term “enterprise risk management.” The insights from his years of helping organizations integrate their risk efforts into the context of their organization’s strategy provide valuable perspectives of tactical approaches that can help to ensure ERM is value-adding. This book helps business leaders see how ERM, if done right, should be an important strategic tool for both management and boards as they strive to enhance the value of the organization for its stakeholders.

—Mark Beasley

Deloitte Professor of ERM and Director of the ERM Initiative

Poole College of Management

North Carolina State University

Raleigh, NC
PRACTICAL ENTERPRISE RISK MANAGEMENT
PRACTICAL
ENTERPRISE RISK
MANAGEMENT

GETTING TO THE TRUTH

Larry L. Baker, CRMA, CCSA, CPA

“…when asked about the value of ERM, one CEO I worked with summed it up in a few simple words: ‘It gets to the truth.’”
# List of Exhibits

<table>
<thead>
<tr>
<th>Exhibit</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exhibit 1.1:</td>
<td>ERM Objectives</td>
<td>12</td>
</tr>
<tr>
<td>Exhibit 2.1:</td>
<td>ERM Framework - Management-Value Approach</td>
<td>20</td>
</tr>
<tr>
<td>Exhibit 2.2:</td>
<td>Risk Management Process</td>
<td>23</td>
</tr>
<tr>
<td>Exhibit 2.3:</td>
<td>Timeline for Risk Management Process Step 1: Risk Assessment</td>
<td>24</td>
</tr>
<tr>
<td>Exhibit 2.4:</td>
<td>Example Enterprise Risk Inventory for the Management-Driven Approach</td>
<td>26</td>
</tr>
<tr>
<td>Exhibit 2.5:</td>
<td>Pre-Read Worksheet</td>
<td>29</td>
</tr>
<tr>
<td>Exhibit 2.6:</td>
<td>Summary of Key Risks</td>
<td>32</td>
</tr>
<tr>
<td>Exhibit 3.2:</td>
<td>Risk Analysis/Action Planning Summary Template</td>
<td>42</td>
</tr>
<tr>
<td>Exhibit 3.3:</td>
<td>Strategic Risk Analysis/Action Planning Detail Template</td>
<td>44</td>
</tr>
<tr>
<td>Exhibit 3.4:</td>
<td>ERM Framework - Management-Value Approach</td>
<td>50</td>
</tr>
<tr>
<td>Exhibit 4.1:</td>
<td>ERM Framework - Board-Confidence Approach</td>
<td>56</td>
</tr>
<tr>
<td>Exhibit 4.2:</td>
<td>Example Risk Inventory with Sample Enterprise Risks</td>
<td>62</td>
</tr>
<tr>
<td>Exhibit 5.1:</td>
<td>Completed Example Enterprise Risk Inventory</td>
<td>68</td>
</tr>
<tr>
<td>Exhibit 5.2:</td>
<td>Inherent Risk Summary Form</td>
<td>70</td>
</tr>
<tr>
<td>Exhibit 5.3:</td>
<td>Environmental, Health, and Safety Example Inherent Risk Summary: Health and Safety</td>
<td>73</td>
</tr>
<tr>
<td>Exhibit 5.4:</td>
<td>Example Executive Summary: Environmental, Health, and Safety</td>
<td>76</td>
</tr>
</tbody>
</table>
Practical Enterprise Risk Management: Getting to the Truth

Exhibit 6.1: Survey Screen Introducing the Survey Criteria ............... 84
Exhibit 6.2: Example Screen of Survey Questions......................... 85
Exhibit 6.3: Enterprise Risks Prioritized................................. 87
Exhibit 6.4: Comparing Priorities by Respondent Group.................. 88
Exhibit 6.5: Enterprise Risk Heat Map.................................. 89
Exhibit 7.1: Grouping of Enterprise Risk for the Inventory.............. 95
Exhibit 7.2: Example Inherent Risk Handout for the Workshop........ 98
Exhibit 7.3: Rating Scale for Workshop Questions......................... 99
Exhibit 7.4: Opportunity Gaps.......................................... 101
Exhibit 7.5: Post-Workshop Survey.................................. 105
Exhibit 7.6: Example Survey Results................................ 106
Exhibit 8.1: Example Executive Dashboard......................... 113
Exhibit 8.2: KPI Framework........................................ 114

All exhibits and templates are available in a format that you can customize to meet the needs of your organization. To access online, please use the following link:

www.theiia.org/practicalERM
The first time I met Larry Baker was in Tulsa, Oklahoma, in 2009. He had invited me to an enterprise risk management (ERM) roundtable that he had organized for business leaders in the region. I was immediately impressed not only by his extensive experience consulting with some very large companies but his ability to articulate a sensible approach to ERM. I came to learn that he was a true pioneer in the field of ERM. I noticed that Larry had a genuine and engaging presentation style that allowed him to communicate complicated ideas in a simple, matter-of-fact way. But, even more than all of that, the trait I observed that most stood out about him was his ability to “get to the truth.”

Since that initial meeting, I have had the pleasure of getting to know Larry quite well and we have collaborated in many different ways. I have been through his training on risk management and internal audit topics. He helped me establish high-functioning, well-respected ERM at a $10 billion energy company. We have been co-workers as well as fellow committee and taskforce members. Larry recently joined The IIA as a member of the Executive Leadership Team. So now, in my volunteer role on the Executive Committee of the Global Board of The IIA, we are working together again to advocate for the profession and help meet the needs of internal auditors around the globe. He seems to inherently know how to modify his style per the scenario and its needs to add value in all of these roles. However, regardless of which hat he is wearing at any particular time, he is always an evangelist for the value of implementing strong risk management.

Larry is intensely adamant about the fact that executing ERM effectively will add value to your organization. Just like me. In fact, as the firm-wide leader of the ERM practice for BKD CPAs & Advisors, one of the nation’s largest professional services firms, I am
now doing much of the same type of consulting that Larry has been doing for years. One of the things I have learned is that executing ERM effectively is not an easy task and the “right” way to implement ERM is different for every organization. Fortunately, Larry’s substantial experience working with executives at many different companies allows him to identify various components of ERM that enable risk managers to create an effective risk management framework regardless of the facts and circumstances.

I have worked for three very interesting Fortune 500 companies throughout my career and all of them have operated in an extremely complex risk environment. A major pipeline company with a brilliant strategy redeployed its previously decommissioned pipelines to be used as conduits for fiber optic cable. The execution of the new subsidiary seemed to be managed relatively well, but too much supply and too little demand eventually led to its bankruptcy, leaving investors with financial losses and many employees with shattered dreams.

One of the largest, most well-managed airlines in the world was responsible for safely flying thousands of passengers around the world at 35,000 feet in a “rocket” filled with jet fuel. However, the economics of competing in an industry where practically all the major players had gone bankrupt was too much to overcome and the airline eventually filed for bankruptcy itself and was acquired by a smaller competitor.

An exploration and production company invested billions of dollars toward exploring for oil or gas hidden deep beneath the surface of the earth in hard-to-reach pockets of rock. The product is highly flammable and under such tremendous pressure that it occasionally explodes and shoots thousands of pounds of steel pipe out of the ground like toothpicks. Then, when fuel prices collapsed, they had to lay off a significant number of employees to continue operating.

What is the common thread that caused all these previously very successful companies to run into financial distress resulting in layoffs and bankruptcies? They all failed to mitigate their business risks in one way or another. They could not get to the truth fast enough. Larry has written this book to help risk managers understand the key components of establishing a successful ERM framework and setting up an effective approach to avoid a similar fate while adding significant strategic value.
I’m sure it’s obvious by now that Larry has the knowledge and experience to address this topic. He is a consummate professional: experienced, knowledgeable, articulate, and, lucky for us, willing to share his learnings with the rest of us. He has a vast repertoire of relevant, useful stories—many of which he has sprinkled throughout this book. One of the characteristics I enjoy most about Larry is his ability to use storytelling to convey difficult and complex concepts.

I am fortunate to call Larry an associate, colleague, and close friend. I commend Larry for taking time to pull together such a practical collection of real-world experiences, tools, techniques, and approaches to facilitate the development and execution of successful ERM. I highly recommend Practical Enterprise Risk Management: Getting to the Truth and predict this book will be required reading for risk managers, chief audit executives, board members, and other executives who desire to make sure their organizations really do “Get to the Truth.”

—Charlie T. Wright, CIA, CPA, CISA
Director, Enterprise Risk Solutions
BKD, CPAs and Advisors
ACKNOWLEDGMENTS

Wow, what an experience, writing this book after 20 years of being in the enterprise risk management (ERM) trenches with courageous colleagues by my side while we pioneered ERM in some of the world’s greatest companies. Having over two decades of success with ERM wouldn’t have been possible without such amazing support of my family, business partners, and friends.

First, I must thank my teenage sweetheart, high school football queen, and wife of over 30 years, Stacy, for her continuous love, support, and understanding as I accumulated over two million airline miles to provide ERM insight and direction to leaders across the world. Second, I don’t have enough space to fully share how proud I am of our three outstanding children, Kyle, 24, Lauren, 19, and Hayden, 13. I cannot ask for a more committed, loving, and successful young man and young woman than what my two older children have grown up to be. And, yes, our youngest is also on a path of success like his big brother and sister. Thanks for loving Dad, even though he traveled much and worked such long nights and weekends at times, more recently including the writing of this book.

Well, Dad, this is a BIG circle! Thank you, Frank Baker, for being a great father who always challenged me, encouraged me, and motivated me to take the world on with passion and confidence. Your motivational sports talks not only impacted my football and baseball careers, they equally impacted my collegiate and business careers. OK, now the hard part, thanking my Mom, who went on to heaven much sooner than we were ready. I know you, Nancy Baker, are smiling down on me, yes, your son who could do no wrong, at least in your eyes! You are the perfect example of what a loving mom should be. Thank you for everything. We miss you, Mom. Also, I want to thank my wonderful parents-in-law, Harry and Linda Dail, who have supported me since I was 16 years old, watched our children when we needed a helping hand, and driven hundreds of miles across the country to watch their grandchildren play sports.
Now on to my colleagues who have worked beside me over the years. Although there are many, I want to mention the few who had a great impact on me as both a professional and a person. First, I must go back to 1992 when my chief audit executive, Jim Mitchell, sent me to Canada to learn about control self-assessment as a fourth-year internal audit professional. What an impact one week had on the rest of my career. Next, I must let some of my closest colleagues and friends know how much I appreciate their support, commitment to success, and long hours we put in together as we exceeded client expectations over and over and over again during our ERM journey—Greg Hopkins, Chris McCarthy, Jeanette York, Rodger Graham, and a host of others. And, most recently, Charlie Wright continues to be a great colleague and mentor who allowed me to bring all my ERM experience to Devon Energy as we jointly developed, evolved, and sustained one of the most effective and efficient approaches to ERM I have experienced over the years. I also greatly appreciate the following colleagues who provided their ERM insights through manuscript review of my book: Tania Stegemann and Angie Chin, along with Greg, Jeanette, and Charlie.

Writing this book would have been impossible without the support of Richard Chambers, Cyndi Plamondon, and Bonnie Ulmer. Thank you for providing me an opportunity to give back to our profession. And, I appreciate your sending me all over the world this year, which allowed me to write much of this book while up in the peaceful blue skies. As for my colleagues at the Internal Audit Foundation and The IIA, our team remained flexible with my busy schedule helping me cross the finish line through effective project management, editing, typesetting, marketing, publishing, and ultimately selling my book. Many thanks to Erika Beard, Lee Ann Campbell, Candace Sacher, Cathleen Kwas, Robert Breen, and Hong Williams. Great job team!

Last, but clearly not least, I want to send a special heartfelt thank you to my new business partner and friend, Jane Seago, right out of my home town, Tulsa, Oklahoma. What an amazing experience it was working with you as you helped me sort through over 40,000 hours of ERM experience and organize my thoughts and experience into one, practical, how-to book. Hey Jane, we did it!
Larry L. Baker, CRMA, CCSA, CPA, is an accomplished and high-impact internal audit and risk management executive with over 40,000 hours of hands-on, real-world enterprise risk management (ERM) experience. He has been a featured speaker and member of The IIA for 30 years, providing thought leadership through global IIA committees, international and national conference presentations, and best practice articles.

Recognized as an early U.S. pioneer of ERM and control-self assessment (CSA), he has teamed with executive management to identify, measure, and report strategic risks and operational issues for many of the world’s largest organizations. Larry also has deep experience with financial and operational audits, COSO frameworks, CSA, and complex company-wide special projects with Fortune 500 companies.

At The IIA, Larry is a member of the executive leadership team. He leads content strategy and retail operations for the Internal Audit Foundation, which provides timely insights that address the needs of our stakeholders globally. He also teams with The IIA’s global leaders to develop The IIA’s global strategic plan.

Prior to joining The IIA, Larry was a senior leader/partner at two Fortune 500 companies, two Big 4 CPA firms, and a global consulting firm. He had the privilege and challenge of building national ERM practices for Deloitte and Ernst & Young, and helping evolve the global ERM practice for Marsh & McLennan/Oliver Wyman. Most recently, Larry led the development and evolution of ERM at Devon Energy, a Fortune 250 company.
INTRODUCTION

Enterprise risk management (ERM) specialists, internal auditors, risk management professionals, and many other leaders help management keep its finger on the pulse of changing and emerging risks in a dynamic world. Although emerging risks can sneak up on an organization with catastrophic impact, equally important are known risks that are changing without appropriate management attention or appreciation. ERM was created to help management meet the challenge by identifying significant risks, effectively managing those risks, and adding value to the organization through better achievement of objectives.

As an early ERM pioneer, I can still vividly remember hearing, “ERM is just another fad you consultants dreamed up to make money.” Well, that was more than 20 years ago and ERM is more alive and well today than ever before. Why? Because when done right, it works.

ERM “done right” means value must be recognized by key stakeholders, including executive management and the board. Some struggle with the challenge of determining how to measure the value of “keeping something bad from happening.” Although I recognize that challenge, I usually take a different approach to measuring ERM value. The value of ERM should be measured on how well we help management manage risks, make better strategic decisions, enhance performance, and achieve objectives that matter most to executive management, the board, and other key stakeholders. Over the years, I have heard many executives, board members, and other stakeholders acknowledge ERM value after seeing the results.

Throughout this book, I will share my real-world experiences and ERM approaches, tools, and techniques that have resulted in better decision-making and generated significant value for some of the world’s greatest companies.
Let me share one of my favorite ERM experiences. A chief operating officer (COO) of a Fortune 500 manufacturing company made a 180-degree turn regarding his view of ERM shortly after the initial step—strategic risk assessment—was completed. When first introduced to ERM, he said, while wringing his hands, “All you risk guys want to do is get us all worried about stuff so we do nothing.” After seeing the results of the strategic risk assessment, he said, “This is all about my business. I will put the best of the best on ERM going forward!” Why? Because we helped him and his executive team “get to the truth” about what risks could have a significant impact on the achievement of his strategic plan that had just been released.

Among several significant risks identified, one was summarized as “potential failure of achieving significant revenue growth due to overreliance on core customers.” The core customers of the company’s recreational products happened to be baby boomers. While the strategies aimed at achieving tremendous growth, the baby boomers were expected to grow too old over time to keep enjoying the recreational vehicles. The COO said, “We thought about threats while developing our plan and we discuss strategies and issues with management continually; however, it took ERM to bring this critical risk to our attention.” Over time, the company developed and implemented meaningful action plans to address the risk and increase the likelihood of achieving projected revenue growth, including modifying their products to attract a more diverse set of customers. Years later, I read an article with the following headline, “Manufacturing Company survives the economic downturn due to diversification of its customers.” That, to me, is real ERM value.

**Why This Book?**

Back in the beginning years of ERM, there was little to no guiding material for us to use. Today, there is an overabundance of ERM material suggesting one approach after another, offering one opinion after another, and providing an endless number of techniques and tools. That is why, after years in the trenches with ERM, I have chosen to write this practical book.
Why will reading this book be useful to you? Most importantly, it is because this book was written by an ERM practitioner for the ERM practitioner and all others who are trying to help their companies manage risks across the enterprise. I have worked in both consulting and the corporate environment acquiring an estimated 40,000 hours of hands-on, real-world ERM experience. I had the privilege and challenge of building national ERM practices for two of the Big 4 CPA firms, helping evolve the global ERM practice of one of the world’s largest insurance brokers, providing ERM services to dozens of Fortune 1,000 companies across industries, and most recently leading the development and evolution of ERM at a Fortune 250 company. Although we all continue to grow with ERM, my experience with initiating, evolving, and sustaining ERM for two decades gives me a good idea of what works and what typically does not work.

Most organizations are aware of the need to get a firm grasp on understanding and addressing their enterprise risks, but many lack an effective, sustainable approach to ERM that has been customized to fit the company culture and management style. Realizing the complexity and velocity of risks in today’s dynamic global environment, those charged with developing, evolving, and leading ERM no longer have time or interest for pure theory, comparisons of generic frameworks, or a recounting of every possible approach to ERM. They need concise, focused, practical help they can begin using almost immediately. I suspect you feel that way too, or you would not have picked up this practical book.

What’s in the Book?

Within these pages you will find no philosophical discussion about the nature of risk or minutely detailed charts of statistics obtained through yet another survey. Instead, you will learn about practical, tested ERM techniques and templates that will help your organization identify significant risks and determine which risks warrant management’s attention. ERM, when done right, provides management ample opportunity to take action to better manage key risks toward achieving the company’s objectives. I will share situations encountered while implementing and leading ERM, lessons learned, and factors that can influence the success of an ERM implementation or evolution.
No one author or one book can possibly tell you everything you need to know about ERM or all the possible ways to implement, evolve, or sustain ERM. To help you know what to expect in the following chapters, provided below are some key points about what this book is and what it is not.

**What it is**

- A “how-to” application of approaches that have worked very well for many organizations of different sizes and industries.
- A step-by-step description of two practical approaches to ERM, including supporting forms, tools, and templates that I have used with multiple companies.
- Customized ERM using terminology preferred by management, some of which may not align with more accepted terminology used by ERM practitioners or highlighted in globally accepted frameworks.

**What it is not**

- A step-by-step implementation of ERM based upon the Committee of Sponsoring Organizations of the Treadway Commission’s (COSO’s) ERM Framework, International Organization for Standardization (ISO) 31000 framework, or any other specific framework.
- A compendium of theoretical tools or sophisticated techniques that “could be” or “should be” used for ERM.
- A summary of an “ideal” ERM approach that claims to be effective for all organizations.

This book discusses proven steps of initiating and evolving sustainable ERM, including activities such as:

- Facilitating an effective strategic risk assessment
- Completing a deeper analysis of broadly stated strategic-level risks
Introduction

• Identifying key risks to the execution of your company’s strategic plan
• Using risk assessment results while developing the strategic plan
• Performing an effective and efficient enterprise risk assessment
• Completing a thorough enterprise risk analysis
• Communicating the most significant risks to executives and the board in a meaningful, actionable way
• Developing a customized and relevant enterprise risk inventory
• Identifying emerging risks through effective risk workshops
• Facilitating development of action plans
• Making practical use of key risks and performance indicators
• Building and sustaining ERM using a customized ERM framework

In short, this book provides practical, how-to instruction on successfully initiating, executing, and evolving ERM.

Who Should Read It?

I realize the range of target audiences for this book is quite broad, both in tenure and level of responsibility. It targets those professionals who are responsible for leading, executing, and evolving ERM, such as chief risk officers (CROs), vice presidents (VPs) of ERM, directors of ERM, ERM specialists, strategic planning leaders, corporate risk managers, and internal auditors. It is also intended to guide those who have an interest in helping management identify, assess, and manage risk across the enterprise and increase the likelihood of achieving company objectives. Regardless of job title and ERM experience, it is possible to learn something new about

Through ERM, we have a great opportunity to help leaders make the best decisions possible, better manage risk, and increase the likelihood of achieving objectives.
ERM every day. I am convinced that there will be something of value for you in the upcoming chapters, whether you are on your first day of being assigned to ERM or you are well into your own ERM journey.

*When,* not *if,* we are successful, we will be contributing to the strategic direction and long-term value of our companies.
CHAPTER 1

SETTING THE STAGE

This chapter covers a variety of topics that are presented, for the most part, in brief, easily digested sections. Each of the topics is critical to understanding this book and successfully implementing ERM.

What Is ERM?

Although ERM has been around for a couple of decades, there continue to be multiple views regarding how it is best defined. One of the definitions I have referenced occasionally is COSO’s. Its most recent definition of ERM is:

“The culture, capabilities, and practices, integrated with strategy-setting and performance, that organizations rely on to manage risk in creating, preserving, and realizing value.”

While that is a good definition of ERM, and one I support, I tend to put it in layman’s terms, especially while talking with management and employees:

“ERM provides timely, useful risk information that helps management make decisions and effectively manage risks toward the achievement of objectives.”

Risk has been around even longer than ERM and continues to be defined in many ways. One definition that I support, also from COSO, is:

“The possibility that events will occur and affect the achievement of strategy and business objectives.”

2 Ibid.
Once again, in practice, many of us try to define risk in its simplest form to facilitate effective discussions with management and employees at all levels. Over the years, I have typically defined risk as “any potential activity or event that could have a negative impact on the achievement of objectives.” This simple definition has been proven effective with executives through front-line employees year after year and company after company. I recognize that risk can have an upside, but in practice, it has been simpler for risk to be discussed with management as a negative event, while considering any upside as an opportunity to better manage a risk toward the achievement of objectives.

For the purposes of this book, enterprise risk is defined as “any significant activity or event that could have a negative impact on achieving objectives across all categories of risk, such as strategic, operational, legal, and financial.” Enterprise risk tends to be more significant to executive management, board members, and other key stakeholders.

This is a good time to share my viewpoint on how to best refer to ERM, and perhaps how not to refer to ERM. I try to limit calling ERM a program or project because both terms sound temporary, with a definite end. I even limit my references to ERM as a process or system because I see ERM ultimately as an integrated part of the business. Finally, I never refer to ERM as a pilot, which tends to infer trying something with hopes it might work. Of course, none of these terms is wrong to use. Ideally, however, I prefer to refer to ERM simply as ERM, with projects being a part of ERM, especially in the early stages of implementation. Leading ERM must be a persistent commitment to proceed and to succeed, no matter how many times you get knocked down along the way—and the terms used to define and describe it must reflect that commitment to long-term success.
Two Proven Approaches

I believe most risks and issues are known among the employees across the organization. The challenge has been, and continues to be, getting those employees to speak up and getting management to listen. My strong belief is that, for most organizations and most risks, somebody, somewhere, knows something. Hence, as risk specialists, we must develop and execute ERM in a way that gets the right information, to the right people, at the right time.

ERM, done right, gives management and employees across the organization ample opportunity to share what they know, in a safe environment, with confidence that management will seriously consider the truth and take action as needed. It is common to discuss ERM at the strategic and executive level. However, I want to emphasize that this philosophy applies at every level of the organization and with every level of employee, from the chief executive officer (CEO) through frontline employees.

Most who have been practicing ERM for many years will agree that there is no “best way” to do it. However, there certainly are some approaches that have been proven effective at well-known companies and private organizations across industries for many years. This book focuses on two such ERM approaches. Before proceeding, I want to provide a little explanation about the titles I chose to use for the approaches:

- The titles are intended to provide a simple way to distinguish one approach from the other as you read about both approaches in the subsequent chapters. Despite the title, most important is for you to understand that each approach requires support from both management and the board.
• The approaches actually have more commonalities than differences. In both approaches:
  - ERM is owned by management.
  - The board provides risk oversight.
  - ERM is focused on objectives.
  - ERM is strategic in nature.
  - It is possible to achieve any of the ERM objectives listed in exhibit 1.1.

Now, let’s summarize the two approaches.

The management-value approach (covered in chapters 2 and 3): The management-value approach tends to be championed by executive management for the primary purpose of creating business value and a secondary purpose of helping the board fulfill its risk oversight role. It generally emphasizes the need to drive value through the identification and resolution of significant residual risks (risks that remain after risk management activities are taken into account) that could hinder the achievement of objectives and goals communicated to shareholders and other stakeholders. As you consider which approach may be best suited for your company, the following ERM objectives (as described in exhibit 1.1) tend to be of highest priority for the management-value approach:

  • **Risk-informed strategic decisions**—ERM helps the organization’s executives make strategic decisions based on consolidated, timely, relevant, and reliable risk information.

  • **Achievement of organization’s strategic objectives**—ERM increases the probability of achieving the organization’s strategic objectives.

  • **Risk-based capital allocation**—ERM provides a process in which capital is allocated considering the risks associated with the investment.

The board-confidence approach (covered in chapters 4 through 7): The board-confidence approach is also championed by executive management but for the primary purpose of helping the board fulfill its risk oversight role and a secondary purpose of creating business value. It generally focuses on gaining board comfort that management
Setting the Stage

understands, communicates, and manages all significant risks to the organization. As you consider which approach may be best suited for your company, the following ERM objectives (as described in exhibit 1.1) tend to be of highest priority for the board-confidence approach:

- **Board comfort and confidence**—ERM provides comfort to the board that it is apprised of the most significant risks potentially impacting creation and protection of shareholder value.

- **Reduced reputational damage and operational surprises**—ERM reduces the occurrence of surprises and noncompliance with laws and regulations through ongoing risk management activities.

- **Portfolio view of risks**—ERM taps into risk knowledge of the organization’s management to provide a consolidated and summarized portfolio view of strategic risks.

Based on my experience, the management-value approach is more commonly used, particularly due to its emphasis on assessing risks against strategic plans and objectives. It is intended to quickly focus on residual risks, whereas the board-confidence approach initially focuses on a holistic view of all critical risks, including risk inherent to the business before considering risk management activities. Both approaches focus on strategic objectives and can work for about any company across industries.

Fully implemented ERM can achieve a number of ERM objectives. I commonly use the 10 ERM objectives shown in exhibit 1.1 to help executive management determine the most important objectives it wants to accomplish with its customized ERM. The order in which the objectives appear in exhibit 1.1 is the order in which I have most commonly seen them ranked by executives across companies and industries. To help you determine the best approach for your company, I recommend you prioritize these objectives in an order that is most appropriate for your executive team and company culture.
### Exhibit 1.1: ERM Objectives

<table>
<thead>
<tr>
<th>Ranking</th>
<th>Objective Title</th>
<th>ERM Objectives</th>
<th>Primary Stakeholders</th>
</tr>
</thead>
<tbody>
<tr>
<td>1st</td>
<td>Board Comfort and Confidence</td>
<td>ERM provides comfort to the board that it is apprised of the most significant risks potentially impacting creation and protection of shareholder value as well as increasing director and officer liability. Consistent process to assess, manage, monitor, and report enterprise risks provides the board with confidence that management is responding appropriately to the most significant risks.</td>
<td>Board/AC Chair, CEO</td>
</tr>
<tr>
<td>2nd</td>
<td>Risk-Informed Strategic Decisions</td>
<td>ERM helps the organization’s executives make strategic decisions based on consolidated, timely, relevant, and reliable risk information. Executives apply risk information in a strategic setting based on a standard risk management process and consistent tools.</td>
<td>Board/AC Chair, CEO, Executive Management</td>
</tr>
<tr>
<td>3rd</td>
<td>Achievement of the Organization’s Strategic Objectives</td>
<td>ERM increases the probability of achieving the organization’s strategic objectives by prioritizing strategic risks and resolving contributing factors directly linked to the achievement of the strategic objectives.</td>
<td>Board/AC Chair, CEO, Executive Management</td>
</tr>
<tr>
<td>Ranking</td>
<td>Objective Title</td>
<td>ERM Objectives</td>
<td>Primary Stakeholders</td>
</tr>
<tr>
<td>---------</td>
<td>------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------</td>
</tr>
<tr>
<td>4th</td>
<td>Reduction of Reputational Damage and Operational Surprises</td>
<td>ERM reduces the occurrence of surprises and noncompliance with laws and regulations through ongoing risk management activities executed at the functional and business process levels of the organization. ERM facilitates timely evaluation and resolution of potentially unfortunate events, thereby minimizing damage to the organization’s reputation, product quality, competitive advantage, and/or financial results.</td>
<td>Board/AC Chair, CEO</td>
</tr>
<tr>
<td>5th</td>
<td>Portfolio View of Risk</td>
<td>ERM taps into risk knowledge of the organization’s management to provide a consolidated and summarized portfolio view of strategic risks that transcend the organization’s operations and support functions.</td>
<td>Board/AC Chair, CEO, Executive Management</td>
</tr>
<tr>
<td>6th</td>
<td>Risk Management Functional Synergies and Efficiencies</td>
<td>Alignment of risk functions’ strategies, goals, and objectives provides synergies and streamlining benefits, thereby reducing costs and minimizing duplicative or conflicting efforts across the organization (e.g., internal audit; legal; human resources [HR]; environmental, health, and safety [EHS]).</td>
<td>Executive Management, Functional Heads</td>
</tr>
</tbody>
</table>
### Exhibit 1.1: ERM Objectives (continued)

<table>
<thead>
<tr>
<th>Ranking</th>
<th>Objective Title</th>
<th>ERM Objectives</th>
<th>Primary Stakeholders</th>
</tr>
</thead>
<tbody>
<tr>
<td>7&lt;sup&gt;th&lt;/sup&gt;</td>
<td>Risk-Based Capital Allocation</td>
<td>ERM provides a process in which capital is allocated considering the risks associated with the investment. Capital investments are pursued on a prioritized portfolio basis, thereby ensuring capital is allocated in the highest priority areas.</td>
<td>CEO, Executive Management, Business Unit Leaders</td>
</tr>
<tr>
<td>8&lt;sup&gt;th&lt;/sup&gt;</td>
<td>Risk-Informed Business Decisions</td>
<td>ERM helps the organization’s managers make daily business decisions based on relevant, timely, actionable, and reliable risk information using flexible risk management processes and tools.</td>
<td>Business Unit Leaders, Managers, Functional Heads</td>
</tr>
<tr>
<td>9&lt;sup&gt;th&lt;/sup&gt;</td>
<td>Achievement of the Organization’s Business Unit Goals</td>
<td>ERM increases the probability of achieving the organization’s business unit goals by identifying key business risks and resolving contributing factors currently hindering the organization’s ability to achieve the business goals.</td>
<td>Business Unit Leaders, Managers, Functional Heads</td>
</tr>
<tr>
<td>10&lt;sup&gt;th&lt;/sup&gt;</td>
<td>Cost Savings</td>
<td>ERM clarifies cost savings and improvement opportunities through execution of risk management plans addressing contributing factors and key root causes such as redundancies, inefficiencies, and waste.</td>
<td>Business Unit Leaders, Managers, Functional Heads</td>
</tr>
</tbody>
</table>

**Who Leads ERM?**

Leaders with various educational and professional backgrounds may lead the ERM charge; however, most important to me is selecting a strong leader who has passion, persistence, and drive. Over the years, I have seen ERM work when championed by treasury, internal audit, strategic planning, risk management, legal compliance, and other departments. Keep in mind that the group that leads ERM tends to apply its
own personal experience and bias. Therefore, ERM may “resemble” the group that designs and implements the approach.

Although ERM could, and probably should, be integrated with strategic planning, it does not mean ERM must be owned or facilitated by the strategic planning group. Just as one example, a Fortune 50 company successfully designed and implemented ERM through the treasury department for more than three years. Shortly after a new chief financial officer (CFO) decided to push ERM ownership over to strategic planning, it lost focus and momentum because the strategic planning leader had limited understanding of ERM and no passion for its success.

The ERM Framework

In this book, I spend considerable time discussing in detail the activities that pertain to each of the two approaches to ERM. While both approaches include activities that constitute a sizable portion of ERM, they are not intended to represent a complete ERM framework. To understand the full picture, the practical steps of ERM should be considered in the larger context of the ERM framework. Each approach’s description begins with a depiction of its customized framework.

The purpose of an ERM framework is to help you, as an ERM champion or implementer, understand what components are necessary to help ERM “live and breathe” and continue to evolve within the company, whether or not you are still involved. In my experience, some ERM components frequently used include governance, infrastructure, integration, and foundation. These key components are necessary to sustain an effective risk management process, which includes steps such as risk assessment, risk analysis, action planning, and risk reporting and monitoring.

Given that the framework is significant to sustaining ERM, it will probably seem counterintuitive when I suggest that you take care not to introduce it too early in your ERM activities. Why? I have found that when it is addressed too early, the ERM effort tends to get lost in philosophical discussions of each element of the framework itself instead of identifying and analyzing significant risks.
Gaining Commitment

To successfully initiate and implement ERM, you must get CEO buy-in and support. Other executives can certainly champion ERM for the organization, but ultimately CEO support is necessary to sustain value-add ERM.

Here is one example of what real-world CEO support looks like. After completing an initial strategic risk assessment, the ERM team presented the top five residual risks to the seven-member executive team of a Fortune 200 railway company. One of those risks was summarized as “potential train derailment.” I remember quite well the COO’s initial response to that particular risk, “Derailment of trains is not a risk; that’s our business!” Well, he was correct, in part. For this company, keeping trains on the track was clearly a key objective, necessary to generate revenue and continue as a business. And he, as COO, had the ultimate responsibility for ensuring that objective was met. However, he also had ultimate responsibility for making sure the risk of derailment was effectively managed, so his peers proactively provided additional insight into why it was a known risk of greater concern than in years past. They pointed out that the company’s trains 1) carried hazardous materials, 2) through largely populated cities, and 3) had recently experienced some minor derailment incidents. Shortly thereafter, the CEO said, “This is a significant risk to our business, and you, COO, will bring an action plan for better managing this risk to me by next month.” No more was said. No more needed to be said. That is what CEO support of ERM looks like.

Successful implementation of ERM, especially in the early stages, is more than getting buy-in; it also requires managing expectations. It is important to be very clear about what executives and management should expect from ERM. For example, I was often asked, “How do you do it and when is it done?” I frequently responded, “Here is how you do it, and there is no ‘done.’”
This was probably not what they wanted to hear, but it was the truth. Remember, many executives are unlikely to know what ERM is all about; they are looking to you for that. I recommend you focus your communication with them on how ERM can help the organization. Explain how identifying and better managing key risks will help the company achieve strategic objectives and corporate goals, as well as the ERM objectives illustrated in exhibit 1.1.

Plain Speaking—Common Language

It is important to keep ERM simple and limit risk jargon as much as possible. Each profession tends to have its own lingo, and using it sometimes signifies that you are a “member of the club.” That is undoubtedly helpful in some situations but not much in ERM, which is most successful when it receives support of management at all levels. Earning that support requires using language that resonates across multiple job titles and levels of responsibility. Using risk specialist jargon can be counterproductive and may alienate employees who have tremendous insight into risks—risks you need to know about.

As you go through the chapters in this book, you will see that we often talk about the importance of using a common language. It is difficult to make progress when every person in a meeting has a different understanding of the topic being discussed. Because executives have often worked in several different companies, they have probably run into different approaches to risk management over time. Chances are good that those approaches used their own language and definitions—reason enough to ensure everyone understands exactly what you mean when you talk about risk and ERM.

I recall one CFO of a Fortune 150 retail company who said, “When risk happens, we are insured.” I knew immediately that this CFO was not ready to embrace the breadth of ERM and its potential to identify and effectively manage a significant risk before it becomes a catastrophic event.
Common ERM Pitfalls

No business practice results in benefits without facing some potential pitfalls along the way. It is important to be aware of what challenges may lie ahead. Here are the most common pitfalls I have seen companies fall into while trying to introduce and evolve ERM:

- Lack of visible, active support from the CEO
- Trying to implement ERM without a framework and a strategic plan
- Overselling ERM’s value, especially during early implementation
- Confusing risk assessment with ERM
- Treating ERM as a project rather than a long-term commitment
- Failing to carry risk management through the entire process
- Failing to realize the need for change management
- Failing to truly integrate ERM into key processes such as strategic planning, capital allocation, and budgeting

Probably one of the most common pitfalls is assigning ERM to the wrong champion. My experience indicates that when ERM fails, it is generally not due to the inadequacy of the activities but of the ERM team itself. Lack of passion or appreciation for all the soft skills necessary to lead ERM trumps even the most proven ERM tools and techniques. So, once you get the support of your executives, it is up to you to execute your plan. The rest of this book will help you do exactly that, so let’s get to work.