Wiley Finance Series

Enterprise Risk and Opportunity Management

Concepts and Step-by-Step Examples for Pioneering Scientific and Technical Organizations

Dr. ALLAN S. BENJAMIN

WILEY

Enterprise Risk and Opportunity Management

Founded in 1807, John Wiley & Sons is the oldest independent publishing company in the United States. With offices in North America, Europe, Australia and Asia, Wiley is globally committed to developing and marketing print and electronic products and services for our customers' professional and personal knowledge and understanding.

The Wiley Finance series contains books written specifically for finance and investment professionals as well as sophisticated individual investors and their financial advisors. Book topics range from portfolio management to e-commerce, risk management, financial engineering, valuation and financial instrument analysis, as well as much more.

For a list of available titles, visit our website at www.WileyFinance.com.

Enterprise Risk and Opportunity Management

Concepts and Step-by-Step Examples for Pioneering Scientific and Technical Organizations

ALLAN S. BENJAMIN

WILEY

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada.

Library of Congress Cataloging-in-Publication Data:

Names: Benjamin, Allan S., author.
Title: Enterprise risk and opportunity management : concepts and step-by-step examples for pioneering scientific and technical organizations / Allan S. Benjamin.
Description: Hoboken : Wiley, 2017. | Series: Wiley finance | Includes index.
Identifiers: LCCN 2016031019 (print) | LCCN 2016055611 (ebook) | ISBN 9781119288428 (hardback) | ISBN 9781119318729 (ePDF) | ISBN 9781119318712 (ePub)
Subjects: LCSH: Risk management. | Information technology—Management. | Strategic planning. | BISAC: BUSINESS & ECONOMICS / Finance.
Classification: LCC HD61 .B46 2017 (print) | LCC HD61 (ebook) | DDC 658.15/5—dc23
LC record available at https://lccn.loc.gov/2016031019

Cover design: Wiley
Cover images: Modern business center, Toronto © PhotoSerg/Shutterstock; Businessman on tight rope © i-works/amanaimagesRF/Getty Images, Inc.

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

Contents

Figures

Tables

Preface

In one form or another, I have been preparing to write this book for many years. In the most recent of those years, my focus has been on collaborating with NASA personnel on producing detailed guidance about potential ways that the agency could apply enterprise risk and opportunity management to help ensure its success as its mission becomes more complex. This collaboration has resulted in the publication of the NASA special publication report, *Organizational Risk and Opportunity Management: Concepts and Processes for NASA Consideration*.

In the process of writing that report, my thinking has evolved into considering two extensions of the original NASA purpose. First is how EROM can be applied to other pioneering technical organizations, both nonprofit and commercial, some of whom I have previously worked with on matters of risk and opportunity assessment and management. Second is how EROM can be integrated with the identification, implementation, and evaluation of internal controls, complying with new requirements from the federal government. This book, therefore, builds on the NASA work by extending it to be generally applicable to organizations of all sorts that are concerned with performing pioneering technical research, integrating and operationalizing that research into complex technical systems, and satisfying externally mandated requirements.

One might ask, "Why yet another guidebook on EROM when there have been several others produced during the past 10 or 15 years?" The answer is that the vast majority of the work that has appeared before now has been oriented toward business and financial organizations, whose objectives center on ultimate monetary gain for their company and their stockholders. In contrast, organizations whose principal objective is to develop and implement risky technologies for scientific and technical gain are faced with different kinds of risks and different kinds of opportunities. In many ways, their risks and opportunities are broader and more challenging than those of the traditional commercial business/financial sector, because their successes may produce breakthroughs that benefit the entire world while their failures may correspondingly have negative global implications. Yet they, like commercial business/financial companies, are also faced with the pressure of tight schedules, decreasing budgets, and political vagaries.

Another reason for writing this book is to fill a gap that exists in explaining how the high-level principles of EROM that others have presented (for example, COSO) can be converted into fine-tuned methods and tools. The practice of EROM in pioneering technical enterprises involves working with mostly qualitative data in a realm that is characterized by high uncertainties. The rigorous part of EROM in such an environment is in the strength of the arguments that are made to reach conclusions about how the enterprise should proceed. Thus, a large part of the effort concerns the derivation of the tasks and templates needed to assist in ensuring that the rationale behind the arguments is both sound and comprehensive. Fulfilling this need is one of the focuses of the book.

Government offices like the office of Management and Budget (OMB), the Government Accountability Office (GAO), and the President's Management Council (PMC) are beginning to encourage and even require the use of EROM in federal agencies, while many top-notch educational and research centers are beginning or have already begun to incorporate EROM into their strategic planning. It is hoped that this book will be of particular value in encouraging and informing these efforts.

In the words of Thomas H. Stanton, past president of the Association of Federal Enterprise Risk Management (AFERM), [quoting from the second quarter 2015 AFERM newsletter]: "Among those agencies that face serious budget cuts, those with strong risk management processes are likely to fare much better—in terms of protecting their core missions and the well-being of their constituents and employees—than those lacking the ability to identify, prioritize, and address major risks that may arise without the protections that effective ERM provides."

Before commencing, I would like to express my special thanks to Dr. Homayoon Dezfuli, Technical Fellow for System Safety and Risk Management at the NASA office of Safety and Mission Assurance, and Chris Everett, Manager of the Technology Risk Management office at Information Systems Laboratories, Inc. (ISL), with whom I collaborated in the formulation of an integrated EROM framework and in the development of the antecedent NASA report through a NASA/ISL blanket purchase agreement (BPA). Special thanks are also due to the following professionals at NASA for reviewing that work and helping to improve its content: Julie Pollitt (retired), Chet Everline, Martin Feather, Sharon Thomas, Emma Lehnhardt, Jessica Southwell (now with the Department of Labor), Prince Kalia, Harmony Myers, Anthony Mittskus, Sue Otero, Wayne Frazier, Kimberly Ennix Sandhu, and Pete Rutledge (retired and now with Quality Assurance and Risk Management Inc.).

Introduction

Enterprise risk and opportunity management (EROM), also known as enterprise risk management (ERM), concerns the means by which organizations apply risk and opportunity considerations in developing their strategic goals and objectives, in implementing them through a portfolio of programs, projects, institutional assets, and activities, and in managing them through internal controls. The overall purpose of EROM is to help reach an optimal balance between minimizing the potential for loss (risk) while maximizing the potential for gain (opportunity).

The principal focus of this book is on the development of an EROM framework and overall approach that serves the interests of organizations that are charged with pioneering the development of new technology and applying it to complex systems (henceforth referred to as "Technical Research, Integration, and Operationalizing enterprises," or TRIO enterprises). The framework is developed first for nonprofit and government organizations whose interests are specifically in achieving technical gains and performing services in the interest of the public. That framework is then extended to provide an EROM framework for commercial TRIO enterprises that develop and apply technology as a means for achieving their stakeholders' financial goals.

The book discusses the philosophical underpinnings of EROM for TRIO enterprises, the integration of EROM with existing management processes, and the nature of the activities that are performed to implement EROM within this context. It also provides concrete examples to illustrate all of these topics. The framework includes a set of core principles and examples that would be pertinent to any successful EROM approach, along with some features that are specific to TRIO enterprises.

The book also provides guidance that is intended to help federal agencies comply with the requirements of the Office of Management and Budget (OMB), expressed in their most recent updates to Circulars A-11 and A-123. The July 2016 update of Circular A-123 directs agencies of the federal government to fully integrate risk management and internal control activities into an EROM framework, proceeding incrementally according to a "maturity model approach." This book discusses organizational structures and analytical tools that are consistent with reaching that point.

Chapters 1 and 2 are intended mainly for high-level managers and their administrative staff who wish to understand the organizational aspects of EROM and the broad concepts of how it could be applied at TRIO enterprises. Chapter 1 is presented in the form of a primer on EROM, answering fundamental questions about how EROM works at a high level, how EROM is particularly relevant to pioneering technical enterprises, how it operates in tandem with existing management structures, how it facilitates interactions with external agencies, and how it can be applied both across the enterprise as a whole and within individual management units of the enterprise. Chapter 2 discusses how EROM coordinates with the major management functions within most technically oriented enterprises, how it helps to shape and corroborate the information that flows within, between, and out of these management functions, how it may be practiced in TRIO enterprises that interact with many partners, both domestic and international, and how it helps to satisfy requirements mandated by governing federal entities.

Chapters 3 and 4 are directed more toward technical managers and practitioners who wish to gain an understanding of some of the more important technical details and the fine points of implementing EROM at TRIO enterprises. Chapter 3 provides guidance on the activities that are conducted within an EROM analysis for TRIO enterprises, including advice on how risk tolerances and opportunity appetites can be established, how risk and opportunity scenarios can be formulated and categorized, how indicators of the potential importance of risks and opportunities can be identified, tracked, and evaluated, how the overall degree of achievement for each objective can be inferred from the indicators, how the potential for unknown and/or underappreciated (UU) risks can be evaluated, how risk and opportunity drivers can be derived, and how responses including risk mitigation, opportunity exploitation, and internal controls can be identified and evaluated. Chapter 4 provides helpful templates for conducting EROM within TRIO enterprises, and using a real example derived from the NASA James Webb Space Telescope (JWST) project, shows how the templates may be populated and exploited for purposes of evaluating overall performance and planning strategy.

Chapter 5 focuses on how EROM may be applied within major technical units of a TRIO enterprise (i.e., technical centers or technical directorates). Sections 5.1 and 5.2 speak about the managerial aspects of EROM at the center or directorate level, emphasizing the various roles that each center or directorate plays in executing its programmatic and institutional responsibilities, the nature of the strategic objectives that require technical centers and directorates to manage multiple partnerships, the ways in which a center or directorate can use an EROM approach to facilitate its management

responsibilities, and the organizational aspects of EROM that permit effective communication between a technical center or directorate and its various partnering organizations. Section 5.3 discusses the technical activities that may be conducted within an EROM analysis for technical centers and directorates, emphasizing the types of risks and opportunities and associated indicators that pertain to its core competencies and the development, allocation, and retirement of its resources and assets. Section 5.3 also provides additional templates, which, together with those in Chapter 4, can be of significant use for planning the strategies and evaluating the overall performance of technical centers and directorates.

Chapter 6 augments the approaches discussed in the preceding chapters to establish a framework for commercial TRIO enterprises, where the primary objectives are the optimization of financial gains for its stakeholders over short-term, mid-term, and long-term time frames. One of the primary intents of Chapter 6 is to incorporate the qualitative aspects of EROM developed in earlier chapters with the quantitative aspects of financial planning and accounting. For this purpose, the treatment of risks and opportunities in the financial model is informed by the risk and opportunity scenarios developed in the templates of Chapters 4 and 5, and the key variables in the financial model are informed by the leading indicators and risk/opportunity drivers identified through the use of the templates. The process is illustrated using, as an example, a fictional prime contractor that manufactures products and develops systems for the aerospace and defense markets. The example focuses on developing risk and opportunity scenario taxonomies and event sequence diagrams that depict the choices that the company has to make and the risks and opportunities that each choice entails with respect to its financial goals. Financially oriented risk and opportunity matrices are introduced to facilitate the decision-making process and the derivation of internal controls.

Chapter 7 deals with the application of EROM results to assist top management in making risk acceptance decisions at key decision points when there are competing objectives at the top level of the organization with correspondingly different levels of risk tolerance. It uses two examples, one based on the DoD Ground-based Missile Defense (GMD) program and the other based on the NASA Commercial Crew Transportation System (CCTS) program, to illustrate the processes involved.

Chapter 8 provides evaluation guidance for independent appraisers who are responsible for auditing the EROM practices and processes employed at a TRIO enterprise and for determining the viability of results obtained from the EROM analyses. The chapter presents a template containing a list of queries whose answers are designed to supply TRIO enterprise management and governing authorities with reliable information about the strength

of the EROM analysis, the robustness of the internal controls relative to the principal risks, and the degree to which reasonable opportunities for progress have been availed. The guidance is intended to be of use to both government and commercial auditors and auditees.

Chapter 9 provides a brief discussion of how EROM in general and the EROM templates in particular can potentially interact with important strategic initiatives and other enterprise-wide activities currently practiced within TRIO enterprises, including technical capabilities assessment (TCA) processes, strategic annual review (SAR) processes, and portfolio performance review (PPR) processes.

Finally, Chapter 10 presents an integrated framework for deriving hierarchies of internal controls based on results from the EROM process. The approach taken here differs philosophically from the approach taken by others (e.g., COSO), where internal controls are derived separately from EROM but used as input to EROM. The fully integrated approach allows for the internal controls to be responsive to the drivers of aggregate risk and opportunity. The hierarchical formulation enables different levels of internal controls to be matched to different levels in the organizational hierarchy. The fully integrated, hierarchical approach is especially suitable for organizations whose objectives are more technical in nature than financial.