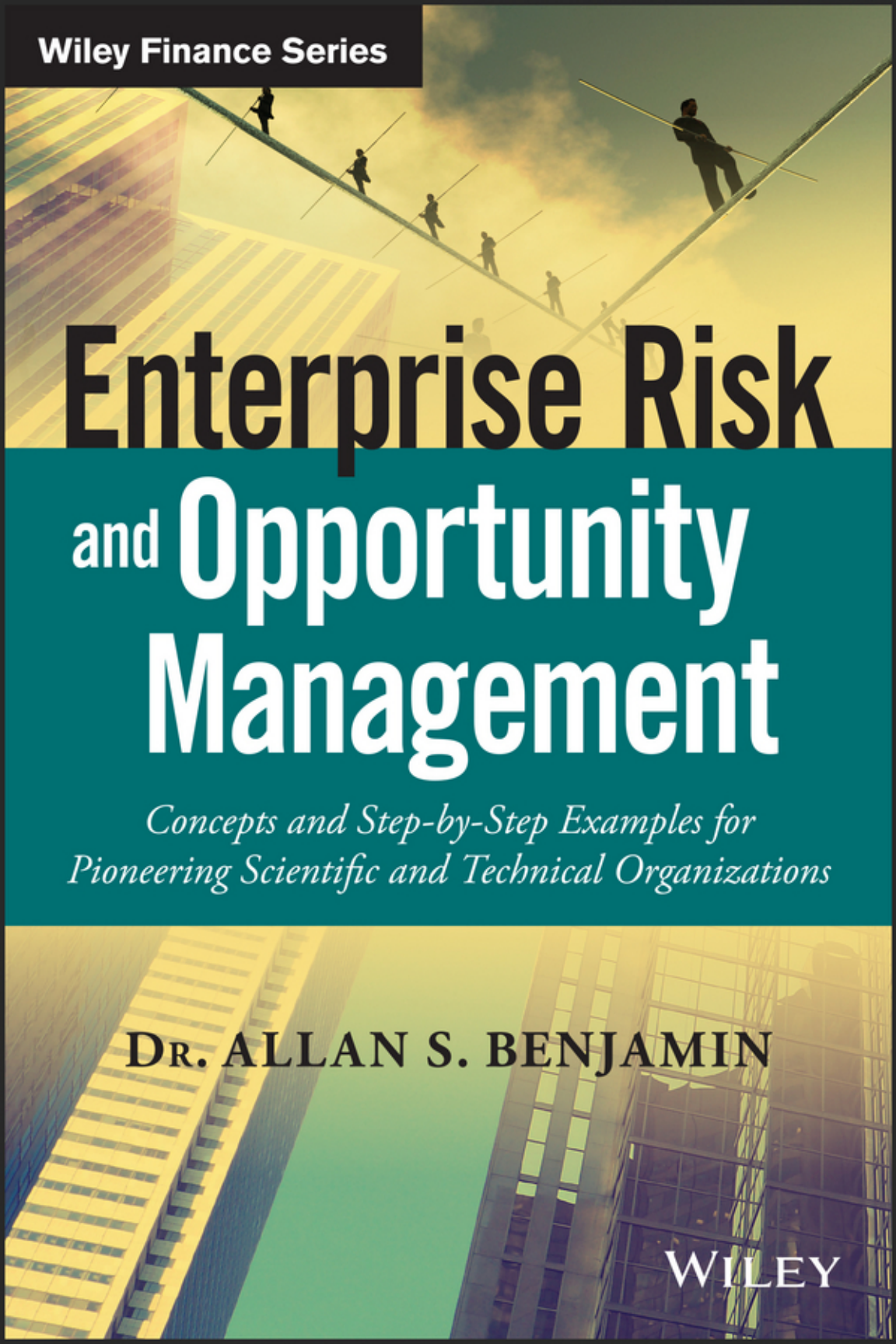




Wiley Finance Series

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

Copyright © 2017 by John Wiley & Sons, Inc. All rights reserved.

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

Published simultaneously in Canada.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise, except as permitted under Section 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 646-8600, or on the Web at www.copyright.com. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at <http://www.wiley.com/go/permissions>.

Limit of Liability/Disclaimer of Warranty: While the publisher and author have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the publisher nor author shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

For general information on our other products and services or for technical support, please contact our Customer Care Department within the United States at (800) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002.

Wiley publishes in a variety of print and electronic formats and by print-on-demand. Some material included with standard print versions of this book may not be included in e-books or in print-on-demand. If this book refers to media such as a CD or DVD that is not included in the version you purchased, you may download this material at <http://booksupport.wiley.com>. For more information about Wiley products, visit www.wiley.com.

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://lcn.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

Preface	xxiii
Introduction	xxv
CHAPTER 1	
An EROM Primer for Organizations Concerned with Technical Research, Integration, and Operations (TRIO Enterprises)	1
1.1 EROM Scope and Objectives for TRIO Enterprises	1
1.1.1 What Is EROM?	1
1.1.2 Why Is EROM Important to TRIO Enterprises?	2
1.1.3 What Kinds of Risk and Opportunity Are Considered within EROM for TRIO Enterprises?	3
1.1.4 How Does EROM for Nonprofit and Government TRIO Enterprises Differ from EROM for Typical Commercial Enterprises?	4
1.1.5 To What Extent Does EROM Work within the Existing Management Structure of a TRIO Enterprise?	5
1.1.6 How Does EROM Facilitate Negotiations between a TRIO Enterprise and the Entities That Provide Funding and Governance?	6
1.1.7 Can Various Management Units within the Organization Separately Apply EROM as Though Each Were an Enterprise?	7
1.1.8 In What Areas Does EROM Facilitate Strategic Planning, Implementation, and Evaluation of Performance for TRIO Enterprises?	8
1.2 EROM Definitions and Technical Attributes for TRIO Enterprises	9
1.2.1 What Is Meant by <i>Risk</i> and <i>Opportunity</i> within the Context of EROM?	9

1.2.2	How Do We Differentiate between Risks and Opportunities during Strategic Planning versus during Plan Implementation and Performance Evaluation?	11
1.2.3	How Does EROM Help Achieve an Optimal Balance between Risk and Opportunity?	11
1.2.4	What Is Meant by the Terms <i>Risk Scenario</i> , <i>Opportunity Scenario</i> , <i>Cumulative Risk</i> , and <i>Cumulative Opportunity</i> ?	13
1.2.5	How Does EROM Incorporate Risk-Informed Decision Making and Continuous Risk Management within the Organization as a Whole and within Different Management Units?	14
1.2.6	Is the Analysis in EROM Principally Qualitative or Quantitative?	16
1.2.7	Can EROM Account for Unknown and Underappreciated (UU) Risks?	17
	Notes	18
	References	19

CHAPTER 2

Coordination of EROM with Organizational Management Activities	21
2.1 The Executive, Programmatic, and Institutional/Technical Management Functions and Their Interfaces	21
2.2 EROM-Relevant Management Activities	23
2.2.1 Activities within Each Management Level	23
2.2.2 Roles and Responsibilities within and between Each Management Level	26
2.3 Coordination of EROM with Management Activities	31
2.3.1 Organizational Planning and Plan Implementation	31
2.3.2 Evaluation of Organizational Performance and Replanning	31
2.3.3 Alignment with Management-Level Roles and Responsibilities	35
2.4 Communication across Extended Partnerships	35
2.4.1 Nature of the Strategic Objectives That Require Extended Partnerships	35
2.4.2 The Challenges of Conducting EROM across Extended Partnerships	42
2.5 Contribution of EROM to Compliance with Federal Regulations and Directives	43

2.5.1	OMB Circular A-11 and GPRAMA (Government Performance, Results, and Budgeting)	43
2.5.2	EROM and Internal Controls from the Viewpoint of Federal Regulations and Guidance	45
2.5.3	OMB Circular A-123 (Management's Responsibility for ERM and Internal Control) and the Required Statement of Assurance	47
2.5.4	Example Risk Profile from OMB Circular A-123	49
	Notes	52
	References	52

CHAPTER 3

	Overview of EROM Process and Analysis Approach	55
3.1	Organizational Objectives Hierarchies	55
3.1.1	Objectives Hierarchies for Each Management Unit	55
3.1.2	Objectives Hierarchy for the Enterprise as a Whole	57
3.2	Populating the Organizational Objectives Hierarchies with Risk and Opportunity Information	61
3.3	Establishing Risk Tolerances and Opportunity Appetites	63
3.3.1	Risk and Opportunity Parity Statements	63
3.3.2	Response Boundaries and Watch Boundaries	65
3.4	Identifying Risk and Opportunity Scenarios and Leading Indicators	66
3.4.1	Risk and Opportunity Taxonomies	67
3.4.2	Risk and Opportunity Scenario Statements	68
3.4.3	Risk and Opportunity Scenario Narratives	72
3.4.4	Risk and Opportunity Leading Indicators	73
3.4.5	Leading Indicators of Unknown and Underappreciated (UU) Risks	74
3.5	Specifying Leading Indicator Trigger Values and Evaluating Cumulative Risks and Opportunities	78
3.5.1	Leading Indicator Trigger Values	80
3.5.2	Cumulative Risks and Opportunities	80
3.6	Identifying and Evaluating Risk Mitigation, Opportunity Exploitation, and Internal Control Options	82
3.6.1	Deducing Risk and Opportunity Drivers	82
3.6.2	Deducing Risk and Opportunity Scenario Drivers	83

3.6.3	Evaluating Risk and Opportunity Scenario Likelihoods and Impacts	85
3.6.4	Identifying Options for Risk Response, Opportunity Action, and Internal Control	87
3.6.5	Evaluating Options for Risk Response, Opportunity Action, and Internal Control	89
3.6.6	Brief Comparison of this Approach with the COSO Internal Control Framework and the GAO Green Book	91
	Notes	94
	References	94

CHAPTER 4

	The Development and Utilization of EROM Templates for Performance Evaluation and Strategic Planning	97
4.1	Overview	97
4.2	Demonstration Example: The NASA Next-Generation Space Telescope as of 2014	99
4.3	Example Objectives Hierarchies	101
4.3.1	Objectives Hierarchies for Different Management Levels	101
4.3.2	Integrated Objectives Hierarchies for the Enterprise as a Whole	103
4.4	Risks, Opportunities, and Leading Indicators	103
4.4.1	Known Risk and Opportunity Scenarios	105
4.4.2	Cross-Cutting Risks and Opportunities	105
4.4.3	Unknown and Underappreciated Risks	112
4.5	Example Templates for Risk and Opportunity Identification and Evaluation	113
4.5.1	Risk and Opportunity Identification Template	113
4.5.2	Leading Indicator Evaluation Template	113
4.6	Example Templates for Risk and Opportunity Roll-Up	126
4.6.1	Objectives Interface and Influence Template	126
4.6.2	Known Risk Roll-Up Template	126
4.6.3	Opportunity Roll-Up Template	144
4.6.4	Composite Indicator Identification and Evaluation Template	147
4.6.5	UU Risk Roll-Up Template	151
4.7	Example Templates for the Identification of Risk and Opportunity Drivers, Responses, and Internal Controls	159
4.7.1	Risk and Opportunity Driver Identification Template	159
4.7.2	Risk and Opportunity Scenario Likelihood and Impact Evaluation Template	161

4.7.3	Risk Mitigation, Opportunity Action, and Internal Control Identification Templates	161
4.7.4	High-Level Display Template	165
4.8	Upward Propagation of Templates for Full-Scope EROM Applications	165
4.8.1	Scope of the Problem	165
4.8.2	Propagation of Templates	173
4.8.3	Development of an Integrated EROM Database	175
4.9	Application of the Templates to Organizational Planning and the Selection from among Alternative Candidate Portfolios	175
	Notes	181
	References	181

CHAPTER 5

Management and Implementation of EROM at the Institutional/Technical Level (Technical Centers or Directorates) 183

5.1	EROM from a Technical Center's Perspective	183
5.2	Extended Enterprises and the Technical Center's Extended Organization	184
5.2.1	Overview	184
5.2.2	Relationship of Each Technical Center to the Other Entities in the Center's Extended Organization	187
5.2.3	EROM Organizational Structure for a Technical Center's Extended Enterprises	189
5.2.4	Challenges of Creating and Managing an Integrated Database	191
5.3	EROM-Informed Budgeting of Resources across a Technical Center's Extended Organization	192
5.3.1	Objectives-Based Distribution of Human, Physical, and Instructional Assets	192
5.3.2	Representative Templates for Distributions of Allocated Assets	192
5.3.3	Asset Risks, Opportunities, and Risk/Opportunity Scenario Statements	198
5.3.4	Leading Indicators of a Technical Center's Health	200
5.3.5	Correlations between Internal Leading Indicators and Gaps in the Distributions of Human, Physical, and Instructional Assets	201
5.3.6	Optimization of the Acquisition, Allocation, and Retirement of Human, Physical, and Instructional Assets	203

5.3.7	Relevance to Provider Acquisition Decisions Made by Technical Centers	206
	References	206

CHAPTER 6

**Special Considerations for EROM Practice and Analysis
at Commercial TRIO Enterprises 207**

6.1	Overview	207
6.2	Risk and Opportunity Scenarios and Leading Indicators	210
6.2.1	Risk and Opportunity Taxonomies	210
6.2.2	Risk and Opportunity Branching Events and Scenario Event Diagrams	210
6.2.3	Risk and Opportunity Templates	215
6.2.4	Risk and Opportunity Matrices	221
6.3	Controllable Drivers, Mitigations, Actions, and Internal Controls	229

CHAPTER 7

**Examples of the Use of EROM Results for Informing Risk
Acceptance Decisions 237**

7.1	Overview	237
7.2	Example 1: DoD Ground-Based Midcourse Missile Defense in the 2002 Time Frame	238
7.2.1	Background	238
7.2.2	Top-Level Objectives, Risk Tolerances, and Risk Parity	239
7.2.3	Risks and Leading Indicators	242
7.2.4	Leading Indicator Trigger Values	244
7.2.5	Example Template Entries and Results	247
7.2.6	Implications for Risk Acceptance Decision Making	247
7.3	Example 2: NASA Commercial Crew Transportation System as of 2015	249
7.3.1	Background	249
7.3.2	Top-Level Objectives, Risk Tolerances, and Risk Parity	251
7.3.3	Remainder of Example 2	253
7.4	Implication for TRIO Enterprises and Government Authorities	254
	References	254

CHAPTER 8**Independent Appraisal of EROM Processes and Results to Assure the Adequacy of Internal Controls and Inform Risk Acceptance Decisions 255**

8.1	Background	255
8.1.1	OMB Motivation	255
8.1.2	Department of Energy Guidance	256
8.1.3	Institute of Internal Auditors Guidance	257
8.2	Queries for an Independent Appraisal of EROM in the Contexts of Internal Control and Risk Acceptance	258
8.2.1	Overview	258
8.2.2	Template for Evaluating EROM Process and Results	259
	References	265

CHAPTER 9**Brief Overview of the Potential Integration of EROM with Other Strategic Assessment Activities 267**

9.1	Technical Capability Assessment (TCA)	267
9.2	Strategic Annual Review (SAR)	270
9.3	Portfolio Performance Review (PPR)	271
	References	274

CHAPTER 10**An Integrated Framework for Hierarchical Internal Controls 275**

10.1	Internal Control Principles and the Integration of Internal Control, Risk Management, and Governance	275
10.2	Methodological Basis	280
10.2.1	Hierarchical Control Loops	280
10.2.2	RACI Matrices	282
10.3	Examples	285
10.3.1	Example 1: Institutional Responsibility for Risk Management and System Safety	285
10.3.2	Example 2: NASA Commercial Crew Program Risk-Based Assurance Process and Shared Assurance Model	287
10.4	Incorporation of Internal Control Principles into the Control Loop Approach	297
10.5	Summary of Observations	302
	References	306

APPENDIX A	
Acronyms	309
APPENDIX B	
Definitions	311
About the Companion Website	314
About the Author	315
Index	317

Figures

1.1	Decision making is a balance between risk and opportunity	12
1.2	Risk tolerance relative to diverse goals and objectives	12
1.3	The elements of RIDM and CRM applied to the TRIO enterprise's management activities at various levels	15
2.1	The three levels of management within a typical enterprise	22
2.2	The principal activities and transfer of information within and between levels of management	22
2.3	Activities within the executive level and transfer of information from/to external and internal sources	24
2.4	Activities within a program directorate (programmatic level) and transfer of information from/to external and internal sources	25
2.5	Activities within a technical center (institutional/technical level) and transfer of information from/to external and internal sources	26
2.6	Interfaces between EROM activities and management activities in the development of an organizational plan	32
2.7	Interfaces between EROM activities and management activities in the evaluation of performance relative to the organizational plan	34
2.8	The relationship between governance, enterprise risk management, and internal controls according to the new OMB Circular A-123	47
3.1	Types of objectives developed at the executive level	56
3.2	Types of objectives developed at the programmatic level	58
3.3	Types of objectives developed at the institutional/technical level	59
3.4	Conceptualization of an enterprise-wide objectives hierarchy	60
3.5	Associating risk and opportunity information with objectives in the organizational objectives hierarchy	62
3.6	Risk and opportunity response and watch boundaries	65
3.7	Example taxonomy for enterprise risks and opportunities	69
3.8	Risk and opportunity leading indicator triggers	81

3.9	Hypothetical results showing how the elimination of a risk driver affects cumulative risk and the elimination of an opportunity driver affects cumulative opportunity	84
3.10	Iterative process for identifying and evaluating a risk response, opportunity action, and internal control plan that balances cumulative risk, cumulative opportunity, and cost	90
4.1	Executive-level objectives for the example demonstration	102
4.2	Programmatic-level objectives for the example demonstration	102
4.3	Center-level objectives for the example demonstration	102
4.4	Integrated objectives hierarchy showing primary interfaces between objectives	104
4.5	Individual risks and associated leading indicators for executive-level objectives	108
4.6	Individual risks and associated leading indicators for program-level objectives	109
4.7	Individual risks and associated leading indicators for center-level objectives	110
4.8	Individual opportunities, introduced risks, and associated leading indicators for executive-level objectives	111
4.9	Secondary objective interfaces for the example demonstration	127
4.10	Schematic of roll-up method alternative 1 for Objective E (>10) #1	131
4.11	Schematic of roll-up method alternative 2 for Objective E (>10) #1	133
4.12	Schematic of risk roll-up for Objective P (1) #11 in the example demonstration	134
4.13	Illustration of risk and opportunity scenario drivers and their time frame criticalities	162
4.14	Illustration of risk and opportunity constituent drivers and their time-frame criticalities	163
4.15	Schematic showing the upward propagation of templates for full-scope EROM applications	174
5.1	The extended organization for a NASA center	186
5.2	NASA example of how each center takes risk and opportunity inputs from a variety of entities and supports multiple strategic objectives of the agency	188
5.3	A representative EROM organizational chart for a technical center that manages extended enterprises	190
5.4	The success of a technical center's inherited strategic objectives is dependent on the "right-sizing" of the resources available to the center (NASA example)	193

5.5	Outline of the steps in the iterative process for optimizing asset distributions based on costs and current and projected values of leading indicators	204
5.6	Illustration of iterative process for optimizing asset distributions based on costs and current and projected values of leading indicators	205
6.1	Integration of qualitative and quantitative modeling to evaluate the likelihood of success of a commercial TRIO enterprise	209
6.2	Example enterprise risk taxonomy for a commercial TRIO enterprise	211
6.3	Example opportunity taxonomy for a commercial TRIO enterprise	212
6.4	Example risk scenario statement and scenario event diagram for a risk in the taxonomic category "Competition from other companies"	213
6.5	Example risk scenario statement and scenario event diagram for a risk in the taxonomic category "Customer satisfaction"	214
6.6	Example risk scenario statement and scenario event diagram for a risk in the taxonomic category "Leadership mortality and succession issues"	216
6.7	Example risk scenario statement and scenario event diagram for a risk in the taxonomic category "Accident causing human deaths"	217
6.8	Example risk scenario statement and scenario event diagram for a risk in the taxonomic category "Changes in foreign exchange rates and interest rates"	218
6.9	Example risk scenario statement and scenario event diagram for a risk in the taxonomic category "Labor strikes"	219
6.10	Example risk scenario statement and scenario event diagram for a risk in the taxonomic category "Exploitation of new technology"	220
6.11	Example risk scenario statement and scenario event diagram for a risk in the taxonomic category "Act of terror"	221
6.12	Example risk and opportunity matrix for quantitative financial objectives	228
6.13	Example risk scenario statement, scenario event diagram, and scenario matrix for a risk in the taxonomic category "Competition from other companies"	230
6.14	Example risk scenario statement, scenario event diagram, and scenario matrix for a risk in the taxonomic category "Exploitation of new technology"	231

7.1	Objectives and hypothetical cumulative risk parity table for GMD example	241
7.2	Risks and leading indicators for GMD example (2002 time frame)	243
7.3	Hypothetical composite leading indicator parity table for GMD example	245
7.4	Objectives and hypothetical cumulative risk parity table for CCTS example	252
9.1	Relationship between the TCA process and the EROM objectives interface and influence template	268
9.2	Relationship between the EROM risk-and-opportunity-based asset optimization process and the TCA asset right-sizing objective	269
9.3	Relationship between the EROM risk and opportunity identification and leading indicator evaluation templates and the SAR process	272
9.4	Relationship between the EROM risk and opportunity roll-up templates and the SAR process	273
10.1	Conceptualization of the relationship between governance, risk management, and internal controls: strategic planning	278
10.2	Conceptualization of the relationship between governance, risk management, and internal controls: organizational performance evaluation	279
10.3	Simplified schematic of the interfaces between organizational management functions and organizational management levels	280
10.4	Standard control loop form	281
10.5	Example simple control loop for a mechanical system	281
10.6	Example form of a hierarchical system of internal control loops	283
10.7	Example primary control loop for the objective of improving risk management and system safety methodology and practice within the enterprise	286
10.8	Process diagram for the selected control activity: “Develop and update risk management and system safety policies, procedures, standards, and guides”	289
10.9	Secondary control loop for the selected control activity: “Develop and update risk management and system safety policies, procedures, standards, and guides”	291
10.10	Process diagram and tertiary control loop for the selected control activity: “Develop and update RM and SS policies, procedures, standards, and guides”	293

10.11 Example primary control loop for CCP's objective of achieving acceptable safety within schedule and budget using the RBA process and shared assurance model	296
10.12 Example generic primary control loop for achievement of internal control principles	304
10.13 Example primary control loop for demonstration of a commitment to integrity and ethical values	305

Tables

2.1	Typical Executive, Program Directorate, and Technical Directorate Managerial Roles and Responsibilities	27
2.2	Executive, Program Directorate, and Technical Directorate Standards of Support to Be Provided by EROM Consistent with Roles and Responsibilities Outlined Previously	36
2.3	Example Risk Profile from the New OMB-Circular A-123	50
3.1	Typical Risk and Opportunity Scenario Types and Associated Leading Indicators	75
3.2	Published Guidelines for Roughly Estimating the Ratio of the System Failure Probability from UU Risks to the System Failure Probability from Known Risks at Time of Initial Operation	79
3.3	Example Likelihood Scale for a Risk or Opportunity Relative to a Critical Organizational Objective	86
3.4	Example Impact Scale for a Risk or Opportunity Relative to a Critical Organizational Objective	87
4.1	A View of the Form of the Outcome for Cumulative Risks and Opportunities	106
4.2	Risk and Opportunity Identification Template	114
4.3	Leading Indicator Evaluation Template	117
4.4	Example Entries for Leading Indicator Evaluation Template for Objective P(1) #11: Deliver the Cryocooler Subsystem	122
4.5	Objectives Interface and Influence Template	128
4.6	Known Risk Roll-Up Template	135
4.7	Example Entries for Known Risk Roll-Up Template for Objective P(1) #11: Deliver the Cryocooler Subsystem	141
4.8	Example Entries for Risk Roll-Up Template for Objective P(1) #11 Including an Intermediate Roll-Up to Risk Scenario Level	142
4.9	Opportunity Roll-Up Template	145
4.10	Example Entries for Opportunity Roll-Up for Objective E(>10) #1: Discover How the Universe Works, Explore How It Began/Evolved, Search for Life on Planets Around Other Stars	148
4.11	Composite Indicator Identification and Evaluation Template	152

4.12	Example Entries for Risk Roll-Up Template for Objective P(1) #11 Using a Composite Indicator	153
4.13	UU Risk Roll-Up Template	154
4.14	Example Risk and Opportunity Driver Identification Template	160
4.15	Example Entries for Risk and Opportunity Scenario Likelihood and Impact Evaluation Template	164
4.16	Example Entries for Risk Mitigation and Internal Control Template for Objective E (>10) #1: Discover How the Universe Works	166
4.17	Example Entries for Opportunity Action and Internal Control Template for Objective E (>10) #1: Discover How the Universe Works	168
4.18	High-Level Display Template	170
4.19	Example Risk Roll-Up Template for the Next-Generation Space Telescope as Applied to Alternative Selection during Organizational Planning	177
5.1	Distribution of Responsibilities among the Principal Entities within the JWST Project	185
5.2	Templates for Distribution of Human (Workforce), Physical, and Instructional Assets	194
6.1	Form of the Risk and Opportunity Identification and Evaluation Templates (Combined) for the Commercial TRIO Enterprise Example	222
6.2	Form of the Risk and Opportunity Roll-Up Templates (Combined) for the Commercial TRIO Enterprise Example	224
6.3	Qualitative/Quantitative Risk and Opportunity Roll-Up Comparison Template for the Commercial TRIO Enterprise Example (Excerpt)	226
6.4	Example Controllable Drivers and Corresponding Existing Safeguards, Risk Mitigations, Opportunity Actions, and Internal Controls for XYZ Company	232
6.5	Excerpt of the Risk Mitigation and Internal Control Template and the Opportunity Action and Internal Control Template for the Commercial TRIO Enterprise	234
7.1	Leading Indicator Evaluation Template for GMD Example (2002 Time Frame)	248
7.2	High-Level Display Template for GMD Example (2002 Time Frame)	249
7.3	High-Level Display Template for GMD Example after Adopting Corrective Actions That Balance the Risks to the Top-Level Objectives	249
8.1	Template for Evaluating EROM Process and Results	259

10.1	Example form of a RACI matrix	284
10.2	Example summary chart of cascading activities, weaknesses, and controls for the SMA organization example	294
10.3	Example RACI chart for the SMA example	295
10.4	Candidates for secondary and tertiary control loops for CCP risk-based assurance process and shared assurance model	298
10.5	GAO green book principles for internal control	299
10.6	GAO green book means of accomplishment for principle 1	300
10.7	MIT-conducted NASA independent technical authority study: system safety principles for internal control and means of accomplishment	301
10.8	Example template for aggregating means of accomplishment to principles	303

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.