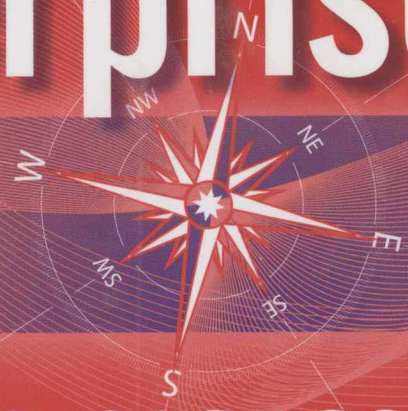
Enterprise Risk Management and COSO



A Guide for Directors, Executives, and Practitioners

HARRY CENDROWSKI and WILLIAM C. MAIR

Enterprise Risk Management and COSO

A Guide for Directors, Executives, and Practitioners

HARRY CENDROWSKI
WILLIAM C. MAIR

John Wiley & Sons, Inc.

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

Published simultaneously in Canada.

Library of Congress Cataloging-in-Publication Data:

Cendrowski, Harry.
Enterprise risk management and COSO : a guide for directors, executives, and practitioners / Harry Cendrowski, William C. Mair.
p. cm.
Includes bibliographical references and index.
ISBN 978-0-470-46065-8 (cloth)
1. Risk management. 2. Corporate governance. I. Mair, William C. II. Title.
HD61.C443 2010
658.15'5—dc22

2009020135

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

About the Contributors

Harry Cendrowski, CPA, ABV, CFF, CFE, CVA, CFD, CFFA, is a founding member of Cendrowski Corporate Advisors, Cendrowski Selecky PC, and The Prosperitas Group. Harry has served as an expert witness in numerous economic damages analyses, contract disputes, lost profit analyses, business valuations, and partnership disputes. He has served as court-appointed receiver in several multimillion-dollar estates, and as the accountant to the trustee in high-profile bankruptcy cases.

Harry is the co-author of *The Handbook of Fraud Deterrence* and *Private Equity: History, Governance, and Operations,* published by John Wiley & Sons, Inc., and has authored articles in several professional publications. These publications include a chapter in *Computer Fraud Casebook: The Bytes that Bite,* a textbook centered on fraud examination.

Along with Jim Martin of CCA, Harry is a co-author of the Certified Fraud Deterrence Analyst (CFD) training materials for the International Association of Consultants, Valuators and Analysts (IACVA). He serves as IACVA's Director of Fraud and Forensic Services. He is also a co-author of the training materials used by the National Association of Certified Valuation Analysts (NACVA) in certifying Certified Forensic Financial Analysts (CFFA).

William C. (Bill) Mair is a director with Cendrowski Corporate Advisors. Bill is the originator of some of the key concepts applied in the structure of the early risk management and control assessment materials. A mathematician and accountant by education, during various phases of his career Bill's roles have included being a military commander, EDP auditor, educator, author, technology consultant, CPA firm partner, professional standards consultant, expert witness, bank internal audit director, insurance company financial executive, corporate director, public investment company trustee, webmaster, and a number of other functions.

The Information Systems Audit and Control Association voted Bill the fourth most influential person among the pioneers of information systems auditing in a study published by *The EDP Auditor Journal*, while his 1972 book, *Computer Control & Audit*, was voted the second most influential

book. Bill is the creator of many systems control concepts and audit techniques now so established as to be viewed as "traditional."

In recent years, Bill has focused on bridging quantitative risk analysis with effective communication to the board level.

Adam A. Wadecki is a manager with Cendrowski Corporate Advisors. Adam specializes in operational analyses, business valuations, and quantitative risk management modeling. He has academic and professional experience in lean manufacturing tenets and the Six Sigma methodology. Adam has helped numerous Fortune 500 companies assess, improve, and monitor the operations of their production facilities. Additionally, in conjunction with the CCA team, he has provided business valuations of publicly traded and private firms that have served as the basis of legal cases, and assisted private equity general partners with their financial due diligence.

Adam is also active in academia. He has authored articles on supply chain management, operational assessments, quantitative risk management, and fraud deterrence, in addition to co-authoring *Private Equity: History, Governance, and Operations*. He has served as a graduate student instructor at the University of Michigan for courses in venture capital finance, private equity, business valuation, and process assessment and improvement.

Adam holds a Master's degree in Operations Research, and graduated *magna cum laude* with Bachelor's of Science degrees in Mechanical and Industrial and Operations Engineering, all from the University of Michigan.

Carolyn H. Rosenberg, Esq. is a partner in Reed Smith LLP's Chicago office. She is a member of the firm's Executive Committee as well as the firm's Audit Committee, and heads the firm's Talent Committee. She frequently advises corporations, directors and officers, risk managers, insurance brokers, lawyers, and other professionals on insurance coverage, corporate indemnification, and litigation matters nationwide and internationally. Carolyn also assists clients in evaluating insurance coverage and other protections when negotiating transactions and represents them in resolving coverage disputes.

Carolyn was selected by *Corporate Board Member* magazine as one of the country's 12 Legal Superstars and the top D&O liability insurance lawyer in August 2001 and she was confirmed as the nation's top D&O liability insurance lawyer by *Corporate Board Member* magazine in a feature on superstar corporate attorneys in July 2004. In addition, Carolyn has been recognized as one of the top lawyers in her field by *Chambers USA 2008–2009: America's Leading Lawyers for Business*.

Efrem M. Grail, Esq. defends entities and individuals in "white-collar" criminal investigations, prosecutions, and administrative enforcement

actions involving allegations of securities, health-care, and business fraud; government contracting, false claims, foreign corrupt practices, and domestic political corruption; and tax and environmental violations. Efrem also litigates complex business disputes, handles injunctions and civil trials in federal and state court, and advises on compliance matters.

A former prosecutor, Efrem has represented clients in confidential matters before federal grand juries and in criminal prosecutions nationwide. He has also represented clients before numerous federal government agencies in administrative enforcement actions.

The Allegheny County Bar Association's Public Service Committee and the Allegheny County Bar Foundation's Pro Bono Center selected Efrem to receive their 2007 Pro Bono Award for Outstanding Individual Attorney and their 2005 Law Firm Pro Bono Award as director of Reed Smith's Pittsburgh pro bono effort. In 2008 and 2009, Efrem was selected for inclusion in *The Best Lawyers in America* in the area of White Collar Criminal Defense. In addition, Efrem has been named a "Pennsylvania Super Lawyer" in the area of White Collar Criminal Defense in 2005, 2006, and 2009.

Acknowledgments

We are sincerely grateful to several individuals for their unique contributions to this book. Adam Wadecki was instrumental in helping us develop ideas throughout the manuscript authoring process. He also assisted us in editing and authoring the manuscript. Adam's contributions helped shape the book that now rests in your hands.

We would also like to acknowledge Carolyn Rosenberg, Esq. and Efrem Grail, Esq. of Reed Smith LLP for contributing a chapter to this book. Their insight into how boards and Chief Risk Officers can quickly identify and contain risks is invaluable to directors whose firms participate in our ever-changing, global environment.

Preface

Recent financial crises have proven that risk management practices are essential for organizations large and small. Publicly traded companies, privately-held firms, and nonprofit organizations were all wounded by the events of 2008 and 2009. Scars from these largely unanticipated or "black swan" events continue to manifest themselves in the growing national unemployment rates, low levels of consumer confidence, and the contracting U.S. gross domestic product (GDP). However traumatic these events have been for our economy, they also provide business leaders and risk practitioners with insights into how we can heal these wounds and prevent them from recurring in the future.

We believe the process of risk management fits within the broader context of organizational management. Risk itself is a driving force in strategic, operational, reporting, and governance decisions. It is a critical cog in the organizational machine—one that can operate with little fanfare, or one that can cause a critical failure. In today's highly competitive world, it is imperative that board members, executives, managers, and employees are involved in the risk management process. The knowledge possessed by each of these individuals allows unique perspectives to be married into a single assessment designed for safeguarding the organization against the many forms of risk.

Until recently, risk management was not generally seen as a component central to the operation of many firms. While detailed risk management activities took place in areas of many organizations, holistic risk management has only recently come into vogue. Many professional organizations such as the National Association for Corporate Directors (NACD) are pushing for significant changes in the way board members and executives evaluate risks. These changes are being made largely in response to recent crises that began in the financial services sector. Indeed, the banking sector is also advocating change in risk management policies with the recent finalization of the Basel Committee's second capital accord (Basel II). While the document was not finalized until 2006, the initial capital accord touched off a discussion on the importance of risk management that began nearly 10 years ago. It is our hope that this text continues this discussion of risk management, highlighting

its importance to directors and executives while also providing insightful information for practitioners.

This book is organized in two sections. In accordance with the aforementioned emphasis on risk management at high levels of the organization, we have grouped material relevant to directors and executives in our first section, "Organizational Risk Management." The second section, entitled "Quantitative Risk Management," is catered to risk management practitioners. We have authored both sections as standalone entities: Readers can elect to focus on either section, or read the book in its entirety.

The first section examines risk management at a macro level. In this section, we emphasize risk management practices most important to board members, C-suite executives (e.g., CEOs and CFOs), and high-level managers. We focus on risk management from a top-down perspective, emphasizing the manner in which executives and directors can cultivate the culture necessary for an organization to possess effective risk management policies. Many pages are spent discussing how these individuals can set an appropriate "tone at the top" that will foster a culture of risk awareness. We have purposefully emphasized understandability over mathematical modeling within this section, given our potential audience members' diverse backgrounds.

The second section details a quantitative framework for analysis that can be used by risk practitioners who perform risk assessments of enterprises, divisions, systems, and processes. This section presents mathematical formulations as well as example assessments of various systems for the practitioner. While the models in this section are mathematical in nature, our goal has been to emphasize practicality over mathematical rigor. The tools illustrated in this section can be employed by practitioners looking for a framework that demonstrates how enterprise risk management policies, similar to those presented in the Committee of Sponsoring Organization's (COSO) Enterprise Risk Management framework, may be implemented.

Our hope is that this book provides a comprehensive resource not only for those in corporate America, but also for individuals in the public sector; risk management practices for governmental organizations are inarguably equal in importance to such practices in private industry.

Many governmental agencies are receiving funds through the American Recovery and Reinvestment Act of 2009 (ARRA). The Obama Administration has made transparency and accountability a primary goal of ARRA in hopes of mitigating risks associated with waste, fraud, and abuse. Decreasing the chance such risks occur will require considerable planning and oversight by administrators, from program inception through conclusion. We believe the quantitative models and framework for analysis contained within this book can help administrators of governmental bodies ensure program goals are achieved, and greater economic impact is realized.

Our risk management framework can also help directors and executives of private companies receiving stimulus funds to mitigate risks. Many private infrastructure companies are receiving major infusions of stimulus dollars for new, capital-intensive projects. Our quantitative models can also assist these firms with mitigating risks associated with cost and time-related overruns that sometimes plague such projects.

Finally, we wish to note that this book is not a comprehensive treatise on risk management techniques or models. Complicated probability models and distributions are not our central focus in this text. Rather, we endeavor to introduce models and risk assessment procedures to the reader that are easily understood and practical in nature. Our goal throughout the authoring process has been to present the reader with a text that is thought provoking, accessible and understandable.

We sincerely hope this book is able to assist the reader in assessing risks irrespective of his or her position or employing organization. We also hope that it will encourage readers to further their knowledge in this essential twenty-first-century discipline.

Harry Cendrowski
William C. Mair
Chicago, IL
September 2009

Contents

SECTION I

Organizational Risk Management

Risk management is a necessary part of our lives. Risk is present in any situation in which decisions must be made under uncertainty with imperfect information. Our minds constantly assess risks as we drive our cars and even pay our bills. In each of these instances, the mind enumerates the risks associated with the activity, quantifies the risk, and then compels us to make a decision based on this assessment.

When operating a vehicle, we are never sure that surrounding drivers will operate their cars in a rational manner. However, we enter such a situation with an *a priori* belief that other drivers are indeed rational. After all, they must pass a test to obtain a driver's license. When we're driving down the road, our minds are continually evaluating and updating this *a priori* belief with respect to every car that is within a personal "envelope of concern."

Driving at a steady speed on the highway, we are not very concerned with the actions of those far behind us. While we can see other cars in the rearview mirror, the likelihood that such a driver's actions impact our own decisions is low. If a far-behind driver loses control, it does not impact us, although it could impact a group of drivers behind us. However, we are very concerned with the actions of those in front of us—most particularly, those immediately ahead of our own vehicle—and those to our side. If these individuals make an error in judgment, the consequences to us could be severe. Our envelope of concern is thus concentrated to the front and sides of our vehicle rather than behind it.

With this simple example we have introduced two central notions of risk assessment: probability and magnitude. The probability that a random driver loses control is identical no matter where this driver is located with respect to us. However, the magnitude of the risk differs based on the location of

the driver. Our minds evaluate both magnitude and probability when we are assessing risks. This assessment is then used to make decisions based on information we perceive. Whether or not we are conscious of it, our minds quantify these risks, and we make decisions based on this quantification.

Although risk management might come naturally to our minds, it is not an involuntary process within an organization. A business must establish, utilize, and monitor risk management procedures to effectively perceive changes in the firm's environment. Returning to our previous example, it is essential that management and board members develop an envelope of concern for the business's strategic objectives. This strategy should focus on risks caused by competitors within the business's immediate operating environment as well as risks posed by potential future competitors, should the organization's environment change.

Organizational Risk Management

Organizational risk management has evolved considerably in the past few decades, from a nascent stage in the 1960s to very complicated modeling in the current day. Risk management within the United States developed primarily in response to the globalization of the U.S. economy. At the turn of the twentieth century, many U.S. businesses focused on selling goods to geographic areas within the country. Few finished goods were imported from overseas or sold across our border. As transportation methods improved in both speed and efficiency through the 1960s, U.S.-based companies began exporting goods abroad. Foreign companies also began selling their goods within the United States.

Prior to this occurrence of global trade, many U.S. industries operated in an oligopoly: The production power of an industry was concentrated within the hands of relatively few corporations. Within such a framework, corporations were able to obtain healthy profits, primarily due to the lack of competition in the marketplace. However, as international competition increased within U.S. markets, the profit margins of manufacturers began to erode. From 1960 through 2008, the U.S. economy shifted from a small net exporter of goods and services to a major importer. (See Exhibit I.1 for more information.) This shift is reflective of the fact that many U.S. corporations began to face increasingly stiff competition from overseas competitors over this time.

Especially susceptible to foreign competition were those manufacturers producing goods with no discernible quality difference from their overseas counterparts. Many U.S. industries began to experience consolidation and hardships that continue today. Witness the current tumultuous environment faced by the U.S. automotive industry and its suppliers as both recently received tens of billions in loans from the federal government.

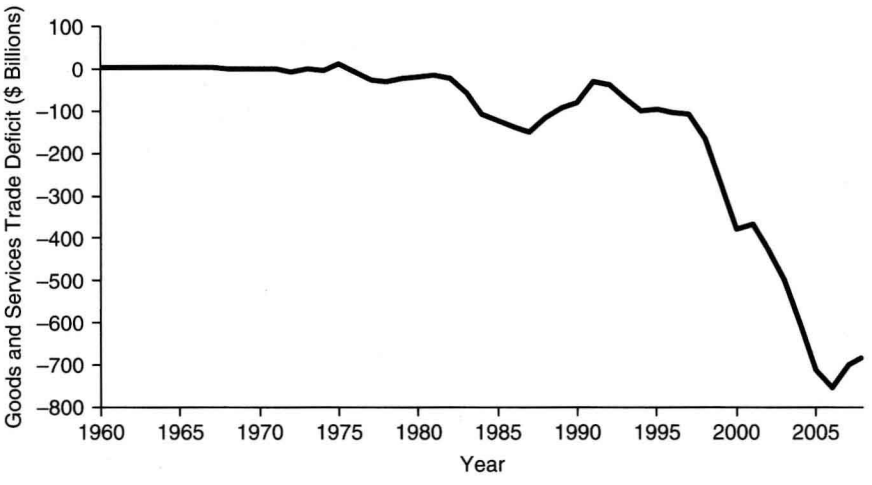


EXHIBIT I.1 Historical U.S. Goods and Services Foreign Trade Deficit, 1960–2008

Source: U.S. Census Bureau.

Modern risk management arose out of this increasingly competitive environment faced by many corporations. In the 1960s, risk management primarily took the form of purchased insurance against *force majeure* events. Today, many corporate executives are worried about not only these types of events but also many others. As shown in the survey results presented in Exhibit I.2, within the United States many corporate chief financial officers (CFOs) are worried about consumer demand and the cost of labor within

EXHIBIT I.2 Top Concerns of U.S. CFOs (Higher Score = Greater Importance)

Rank	Concern	Avg. Importance Score
1	Consumer demand	0.82
2	Cost of labor	0.73
3	Credit markets/interest rate	0.59
4	Cost of fuel	0.58
5	Cost of health care	0.56
6	Housing-market fallout	0.50
7	Skilled-labor shortage	0.48
8	Regulation	0.39
9	Cost of nonfuel commodities	0.30
10	Currency values	0.27

Source: Duke University/*CFO Magazine Global Business Outlook Survey*.

the United States.[1] Natural disasters—a primary subject of risk managers 40 years ago—did not even make the list of CFO's top concerns.

Contemporary risk management takes the form of hedging against shocks in the currency, stock, and commodities markets; evaluating organizational strategy, reliability of financial reporting, and risks in operations; and assessing risks in corporate governance procedures. Accordingly, many professional standards that focus on risk management have been introduced within the past two decades.

In 1995, Standards Australia published one of the first modern risk management standards with AS/NZS 4360: 1995. Canada soon followed suit in 1997 with the publication of CAN/CSA-Q850-97, as did the Institute of Chartered Accountants in England and Wales with their Turnbull Report, released in 1999. This latter standard called for stronger internal controls in financial reporting and better monitoring of risks throughout the organization.

Risk management standards within the United States largely took a back seat until the financial scandals of the 2000s (involving Enron, WorldCom, and Tyco, among others). These events forced the passage of the Sarbanes-Oxley Act of 2002 and in 2004 led to the creation of the enterprise risk management (ERM) framework by the Committee of Sponsoring Organizations (COSO). This latter framework will serve as the foundation of our risk management methodology introduced in the second section of our book.

The Risk Assessment Process

The risk assessment process consists of five steps:

1. Enumeration of risks
2. Qualitative analysis
3. Quantitative analysis
4. Implementation of risk management strategy
5. Assessment of risk management strategy

Risk assessment in organizations is the domain not only of the auditor but of operating managers, board members, and C-level executives. As stated in the Preface, all four of these groups comprise the intended audience for this book.

Auditors assess risks when they perform an examination (commonly called an "audit" when it involves financial statements). In performing an examination, an auditor must select a combination of information from a large body of evidence that limits the risk of a material misstatement. Operating managers must assess risks associated with the internal operations of the business. If performance metrics begin to indicate that the organization

is struggling to achieve its mission, managers must prioritize initiatives according to the risks they pose to the organization's health. C-level executives examine risks to the organization's strategic plan from external and internal threats. This also falls within the domain of the board of directors.

Risk Management at the Board Level

The recent economic crisis has put a renewed emphasis on directors' oversight over the day-to-day operations of their organizations. In the words of the National Association of Corporate Directors (NACD), the board:

> *is charged with selecting and evaluating senior executives; planning for succession; monitoring performance; overseeing strategy and risk; compensating executives; approving corporate policies and plans; approving material capital expenditures and transactions not in the ordinary course of business; ensuring the transparency and integrity of financial disclosures and controls; providing oversight of compliance with applicable laws and regulations; and setting the "tone at the top."*[2]

This is no small order for individuals who often serve as executives at other companies. Though this list of responsibilities is rather long, all its elements essentially fall under a single umbrella: risk management.

Although directors must principally look out for the interests of shareholders, they are also accountable to employees, regulators, suppliers, and customers. Balancing responsibilities to these individuals is no simple task. In the words of the NACD, "Serving as a director is demanding and—in addition to significant substantive knowledge and experience relevant to the business and governance needs of the company—requires integrity, objectivity, judgment, diplomacy, and courage."[3] Moreover, shares of many organizations are held by diverse groups of investors, including individual investors, pension funds, hedge funds, and university endowments. Each of these investors may have different investment horizons, expectations of returns, and opinions on risks the organization should bear in generating returns. Catering to each of these investors can prove difficult without a proper risk management plan.

Sound risk management practices enable board members to fulfill their fiduciary obligations to all stakeholders of the organization. Such practices ensure that information systems properly assimilate data from different parts of the organization, that this data is critically analyzed, and finally, that plans are verified or modified because of the data. Performance measurement, strategic goal setting, and establishment of corporate policies are all outputs of this process, the result of which is increased value for all stakeholders.