

北京大学、中国人民大学会计学权威联合推荐

审计人员 风险管理指南

审计与企业风险管理的结合

[美] 保罗·J·索贝尔 (Paul J. Sobel) / 著

Auditor's Risk
Management Guide

Integrating
Auditing and

ERM



本馆附光盘



中信出版社
CITIC PUBLISHING HOUSE

北京大学、中国人民大学会计学权威联合推荐

审计人员 风险管理指南

F239-62

Y1

2004

审计与企业风险管理的结合

[美] 保罗·J·索贝尔 (Paul J. Sobel) / 著

Auditor's Risk
Management Guide

Integrating
Auditing and
ERM



中信出版社
CITIC PUBLISHING HOUSE

图书在版编目 (CIP) 数据

审计人员风险管理指南 / [美] 索贝尔著. —影印本. —北京: 中信出版社, 2003.12

书名原文: Auditor's Risk Management Guide: Integrating Auditing and ERM

ISBN 7-80073-974-0

I. 审… II. 索… III. 审计-风险管理-指南-英文 IV. F239-62

中国版本图书馆CIP数据核字 (2003) 第102094号

Auditor's Risk Management Guide: Integrating Auditing and ERM by Paul Sobel

Copyright © 2003 by Aspen Publishers, Inc.

This volume of *Auditor's Risk Management Guide*, by Paul Sobel, is an English Reprint Edition meant solely for publication in the country of China, published and sold by CITIC PUBLISHING HOUSE, by permission of ASPEN PUBLISHERS, INC., New York, New York, U.S.A., the owner of all rights to publish and sell same.

本书由中信出版社与Aspen Publishers, Inc.合作出版, 未经出版者书面许可, 本书的任何部分不得以任何方式复制或抄袭。

审计人员风险管理指南: 审计与企业风险管理的结合

SHENJI RENYUAN FENGXIAN GUANLI ZHINAN

著 者: [美] 保罗·J·索贝尔

责任编辑: 李 莎

出版发行: 中信出版社 (北京市朝阳区东外大街亮马河南路14号塔园外交办公大楼 邮编 100600)

经 销 者: 中信联合发行有限公司

承 印 者: 北京牛山世兴印刷厂

开 本: 787mm × 1092mm 1/16 印 张: 33.75 字 数: 506 千字

版 次: 2004年1月第1版 印 次: 2004年1月第1次印刷

京权图字: 01-2003-6043

书 号: ISBN 7-80073-974-0 / F·638

定 价: 59.00元 (含光盘)

版权所有·侵权必究

凡购本社图书, 如有缺页、倒页、脱页, 由发行公司负责退换。服务热线: 010-85322521

E-mail: sales@citicpub.com

010-85322522

中文版序

以一句很多人使用的话说，会计行业近两年正处于争论的漩涡之中。

2001年以来，美国爆发一系列财务虚假案，使得安然、世通等巨型公司破产，也导致安达信这样一个有着九十多年历史的世界级会计师事务所饱含屈辱地退出审计市场。安然和世通等事件的影响巨大，损失了几十亿美元的价值。人们开始质疑，这些巨人公司的账面价值到底在多大程度上是真实的？事实上，公众对这种价值创造所依赖的会计和财务制度的信任已经动摇。为了重树公众信心，美国制定颁布了《公众公司会计改革和投资者保护法》（Public Company Accounting Reform and Investor Protection Act of 2002），简称为《萨宾纳斯—奥克斯莱法案》（Sarbanes-Oxley Act），对美国而且对世界各国会计、公司治理以致整个证券市场，都产生了相当大的影响。

在中国，上述问题也一样沉重。由于与会计信息相关的违规行为而被证监会查处，或被沪深证交所公开谴责和批评的上市公司，已经是越来越多。在一张张让人不放心的公司财务报表面前，公众感到疑惑，无所适从。银广夏和中天勤案件的查处，让会计师和注册会计师面临空前的信任危机，会计和审计专业的信誉面对巨大的挑战。

在会计信息和资本市场问题上，存在着一个“公司财务报告供应链”。谁组成了公司财务报告供应链呢？毫无疑问，公司财务报告供应链启动于公司内部管理层，他们是原始会计信息的拥有者，他们负责编制和向投资者与其他利益相关者提供财务报表，并承担会计信息质量的最终责任。实务中，会计报表和财务报告由CFO领导下的公司财务报告系统编制，由CPA进行独立审计鉴证，经过董事会批准和股东大会通过后予以公布，还要由证券分析师进行分析，由媒体进行信息传播。在获得上述直接和间接财务信息的基础上，投资人和其他利益相关者做出自己的决策。

显然，这个长长的公司财务报告供应链由许多环节组成，每个环节都有不同的供给方和需求方。

从公司财务报告供应链的视角看，应该说，财务信息的可靠性是由链条中的所有各方共同保证。当然，社会和公众有理由对链条中最为重要的两个环节——会计师和审计师——提出更高、更严格的要求。会计师和审计师必须在具备诚信度的同时，把透明度和受托责任奉为职业要素。

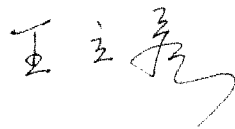
写了以上几段话，是为了引出对本套中信财会图书馆影印系列专业书籍的认识和介绍。这套系列丛书包括12本书。大体上可以归为三类：

第一类：《会计案头必备：财会人员日常速答手册》、《金融工具——会计及财务报告综合指南》、《商业企业与工业企业财务比率年鉴》、《购买和出售企业专业指南：税收、价值评估、法律和会计核算》、《启动财务——企业初创阶段筹集资金指南》。这几本书的内容聚焦于企业会计和财务管理人员的日常专业工作。

第二类：《审计委员会——公司董事、管理层以及咨询人员指引》、《会计违规和财务欺诈》、《审计程序》、《审计人员风险管理指南：审计与企业风险管理的结合》。这几本书的内容聚焦于审计方面，维护财务信息质量是共同主题。

第三类：《欧洲会计指南》、《国际会计准则指南》、《FASB准则的再阐释与分析：GAAP指南》。这几本书的共同主题是会计规范。

总而言之，这12本书是一套财会方面的好书，既包含有详细的专业规范，又包含了丰富的实务经验，具体应该特别指出以下重要话题：其一，与公司治理有关的机制问题，《审计委员会——公司董事、管理层以及咨询人员指引》非常值得细读；其二，有关《萨宾纳斯—奥克斯莱法案》的问题，在《会计案头必备：财会人员日常速答手册》一书中专设一章“The Sarbanes-Oxley Act of 2002”予以介绍；其三，《购买和出售企业专业指南：税收、价值评估、法律和会计核算》、《启动财务——企业初创阶段筹集资金指南》等书的主题，不在会计、审计方面，而是专项财务管理；其四，我国会计界对英美制度关注比较多，而对欧洲国家的会计制度了解很少，对此，阅读《欧洲会计指南》会有收益。



2003年初冬
于北京大学光华管理学院

About Aspen Publishers

Aspen Publishers, headquartered in New York City, is a leading information provider for attorneys, business professionals, and law students. Written by preeminent authorities, our products consist of analytical and practical information covering both U.S. and international topics. We publish in the full range of formats, including updated manuals, books, periodicals, CDs, and online products.

Our proprietary content is complemented by 2,500 legal databases, containing over 11 million documents, available through our Loislaw division. Aspen Publishers also offers a wide range of topical legal and business databases linked to Loislaw's primary material. Our mission is to provide accurate, timely, and authoritative content in easily accessible formats, supported by unmatched customer care.

Accounting Research Manager

Aspen Publishers' Accounting Research Manager™ is one of the largest and most comprehensive online databases of expert-written analytical accounting and auditing information as well as primary source data. Updated daily, it is the most timely, complete and objective resource for your financial reporting needs. Our Weekly Summary, an e-mail newsletter highlighting the key developments of the week, gives you the assurance that you have the most current information. It provides links to all FASB, AICPA, SEC, EITF, and IASB authoritative and proposal-stage literature, plus insightful guidance from financial reporting experts. With Aspen's Accounting Research Manager, you maximize your research time, while enhancing your results. Visit us at www.arm.aspenpublishers.com to request your free 30-day trial.

To order any Aspen Publishers title, go to www.aspenpublishers.com or call 1-800-638-8437.

To reinstate your manual update service, call 1-800-638-8437.

For more information on Loislaw products, go to www.loislaw.com or call 1-800-364-2512.

For Customer Care issues, e-mail CustomerCare@aspenpublishers.com; call 1-800-234-1660; or fax 1-800-901-9075.

Aspen Publishers
A Wolters Kluwer Company

Preface

One only needs to pick up the newspaper to be reminded of how ineffectively managed risks can send shock waves through the equity and capital markets. The list of bankruptcies, frauds, and accounting irregularities continues to grow with each passing week. Confidence in accountants and auditors is lower than at any time in recent memory.

So, why does the business world need another book about auditing? That's a question I asked myself several times while writing this book. However, I believe that in light of recent events and legislation, boards and audit committees will be asking auditors how they plan to adjust their approach. There is an opportunity, and more so a need, for auditing to evolve along side leading edge management practices, and help restore confidence in the value auditors can provide. The audit approaches of the past will not be sufficient to meet the needs of the future.

With the boom of risk-based approaches in the 1990s, auditing, whether internal or external, was viewed as more relevant and valuable than in the past. Auditors began focusing resources on the risks that could impact financial reporting and internal controls, instead of the financial balances themselves. However, as the decade progressed, many business executives began embracing Enterprise Risk Management (ERM) concepts, which focus on a broader array of risks than those covered by traditional risk-based auditing. Therefore it has become necessary for risk-based auditing to evolve in order to keep up with the way executives are thinking and managing businesses today.

As my understanding and appreciation of ERM principles increased, I realized that these principles could also be applied to auditing approaches, thus creating a superior methodology that retained the flexibility and ease of execution that past methodologies employed, while further reinforcing the value of auditing to executives. This new approach, called Risk Management-Based Auditing, integrates key ERM concepts with previous audit methods by:

- Embedding strategy and objectives in the planning of the audit, positioning them as the foundation for audit judgments.
- Recognizing that audit judgments should be based not only on the auditor's tolerance for risk (as was the case in the past), but also on management's tolerance for risk in the area.
- Increasing the focus on how management measures and monitors performance relative to their objectives and tolerances.
- Evaluating the organization's abilities to manage risks on an ongoing basis, instead of focusing only on their success in managing risks in the past.

- Establishing a basis by which auditors can provide management and the board with assurances regarding the effectiveness of risk management and governance activities.

At first blush, some of these concepts may not sound like significant advances. However, when integrated with existing fundamental auditing principles, the result is a powerful, yet flexible approach to auditing any financial account, process, control, system, objective, transaction, initiative, or whatever one wants to audit. Risk management-based auditing concepts can be applied to virtually any project or decision-making activity.

How This Book Is Organized

Auditor's Risk Management Guide: Integrating Auditing and ERM is designed to be a comprehensive "how-to" book that provides the reader with guidance on performing a risk management-based audit. This is not a research study or a conceptual thesis; rather, it is a practical guide designed for the audit practitioner. It is organized into two parts: Part I, "Risk Management-Based Auditing" and Part II, "Case Studies."

The first three chapters in Part I provide the reader with a broad understanding of corporate governance, ERM principles, and the different auditing approaches. These chapters establish the foundation and relevance for risk management-based auditing. The next three chapters outline the approach for understanding the strategy and risks inherent in the business. These chapters create the framework for annual audit planning and linkage to the company's overall strategy. The remaining seven chapters in Part I provide step-by-step instructions on how to execute the risk management-based audit methodology. The Practice Pointers and Observations provide additional commentary to assist the reader in understanding the methodology. Additionally, examples from a fictional company, AfterMath, Inc., bring the methodology to life by building on examples in previous chapters.

Part II, the "Case Studies" section of the book, presents nine detailed case studies, beginning with a business risk assessment and working through common audit areas, such as accounts payable and accounts receivable. These in-depth case studies illustrate the risk management-based audit methodology and tools in different audit scenarios, helping the reader understand how the methodology can be applied in strong, moderate, and weak risk management areas.

Finally, a CD-ROM is included with the book that provides an electronic version of the various work programs, checklists, and other tools illustrated throughout the book. The programs and checklists are presented in a question format to help the auditor understand what questions need to be asked and answered as they execute the

methodology. These tools will help the auditor begin applying the methodology immediately, eliminating the need to develop the tools on their own.

Although many readers will read the "Risk Management-Based Auditing" chapters completely before looking at the case studies, some readers may find it helpful to review the examples in the case studies after each chapter in order to reinforce the concepts discussed in the methodology. These readers then may want to look at the tools, which are referenced by Exhibit or Illustration number on the CD-ROM Contents, to appreciate how easy it is to use the tools.

Regardless of how readers choose to navigate the book, it is organized in such a way to provide both the understanding and examples necessary to execute the methodology.

Acknowledgements

An undertaking of this magnitude certainly requires the help and support of a great many people. First and foremost, I am grateful to my wife Colleen, who provided me support and encouragement throughout, and helped me find the time to write by keeping the kids busy during blocks of time on the weekends and evenings. Her love and support kept me going. I thank my children, Lauren, Corey, and Briana, who left me alone when I needed to concentrate on the book, and never complained that they didn't get to spend enough time with their daddy. Because of my family's ongoing encouragement and excitement about this book, I dedicate it to them.

I acknowledge my team here at Aquila, without whom these concepts could ever have been tested. I thank Cal, my boss, for the encouragement to undertake the project. I thank Lynn and Susan, my Managers, who played the healthy skeptics and pushed back when one of my ideas didn't make sense or didn't work in a real audit. I thank Barb for helping me think through the early concepts that would make up this methodology, and Kurt for helping me expand my understanding of how ERM concepts align with corporate governance. I thank James, Dawn, Keith, John, and Tony, who were all willing guinea pigs in testing out the methodology on different audits, and provided me with valuable advice on how to sharpen the approach.

I must also say thanks to my friends at what was once Arthur Andersen. Deanna, Tammy, and Terry helped challenge and inspire me on the many firm-wide projects we attacked together. Jim helped provide me with the conceptual foundation for ERM through his book, and Dan helped me apply some of these concepts in client engagements. And I want to add to this list the many partners, in Kansas City and around the world, who gave me the opportunity and support to pursue these fascinating and ambitious projects. Thanks to you all.

Finally, I thank Mark and the team at Aspen Publishers. Mark picked me out from the many speakers he heard at different conferences and convinced me that there was a market for a practical, how-to book on this subject. His ongoing support kept me excited about this project during the many months that it took to complete. This book would not have been possible without the experience of such a publisher standing behind me as an author.

*Paul J. Sobel
Overland Park, Kansas*

About the Author

Paul J. Sobel, CPA, CIA, has more than 20 years of auditing experience at three Fortune 500 companies and a major international public accounting firm. He is currently Vice President, Risk Assessment, for Aquila, Inc., an international energy company based in Kansas City, Missouri. His responsibilities include developing and implementing Aquila's Enterprise Risk Management program and directing the company's internal audit activities. He is a frequent speaker on ERM topics at conferences around the country and achieved Distinguished Faculty honors as an instructor of seminars for the Institute of Internal Auditors.

During his career with Arthur Andersen, Paul gained extensive experience performing and managing financial statement and risk-based internal audits. He was active in firm-wide initiatives, including the development of the firm's risk assessment methodology and training. He also contributed to and instructed the firm's risk consulting essentials course, and participated in the development of a risk management diagnostic tool.

Paul's career has also included the Audit Director position at Harcourt Brace publishers in Orlando, Florida, and the International Audit Manager position with PepsiCo, based out of Purchase, New York. He is a graduate of Washington University in St. Louis, Missouri, and is active in the Institute of Internal Auditors, both at the national and local levels.

Contents

<i>Preface</i>	vii
<i>About the Author</i>	xi

PART I: RISK MANAGEMENT-BASED AUDITING

Chapter 1: Overview of Enterprise Risk Management	1.01
Chapter 2: The Enterprise Risk Management Funnel	2.01
Chapter 3: Evolution of Auditing Approaches	3.01
Chapter 4: Strategy—The Beginning of the Journey	4.01
Chapter 5: Risk Assessment—Business Level	5.01
Chapter 6: Risk Assessment Quantification Techniques	6.01
Chapter 7: Risk Assessment—Process Level	7.01
Chapter 8: Process Design Phase	8.01
Chapter 9: Testing Phase	9.01
Chapter 10: Risk Infrastructure Assessment	10.01
Chapter 11: Action Planning Phase—The Real Value	11.01
Chapter 12: Monitoring and Follow-Up	12.01
Chapter 13: Auditing the ERM Process	13.01

PART II: CASE STUDIES

Chapter 14: Case Study—Business Risk Assessment	14.01
Chapter 15: Case Study—Risk Management Infrastructure	15.01
Chapter 16: Case Study—Inventory	16.01
Chapter 17: Case Study—Procurement	17.01
Chapter 18: Case Study—Accounts Payable and Disbursements	18.01
Chapter 19: Case Study—Accounts Receivable and Collections	19.01
Chapter 20: Case Study—Quality Assurance	20.01
Chapter 21: Case Study—Payroll and Related Liabilities	21.01
Chapter 22: Case Study—Fixed Assets	22.01

<i>Index</i>	I.01
--------------	------

CHAPTER 1

OVERVIEW OF ENTERPRISE RISK MANAGEMENT

CONTENTS

Introduction	1.01
Risk Defined	1.02
The Transformation to ERM	1.02
The Underlying Impetus	1.03
Fundamental ERM Techniques	1.04
The Role of ERM in Corporate Governance	1.05
Corporate Governance Defined	1.05
The Corporate Governance Cycle	1.06
Stakeholders	1.07
Corporate Governance Umbrella	1.07
Enterprise Risk Management Process	1.08
Risk Management Activities	1.09
The Continuous Cycle	1.10
The Future of Enterprise Risk Management	1.12
Summary	1.13
Exhibit	
<i>Exhibit 1-1: Corporate Governance Cycle Checklist</i>	1.14

INTRODUCTION

Most risks are managed in the business world in much the same way as life—they are managed instinctively by experienced and talented people, most of whom either already know or figure out how to avoid undesirable outcomes. However, although management by instinct has proven to be generally effective throughout the ages, in today's competitive environment companies cannot afford to rely solely on instincts for success.

This opening chapter focuses on providing the reader with an understanding of risk and how risk management concepts have evolved. It discusses risk, enterprise risk management (ERM), and corporate governance. This overview serves as a basis for concepts

used throughout the entire book. It provides the foundation for understanding enterprise risk management, and how auditors can effectively add value when auditing in an ERM environment.

RISK DEFINED

Businesses must deal with risks, many of which have the same characteristics as those encountered in other parts of life. To put risk in the proper business context, *business risk* is defined for purposes of discussions throughout this book as follows:

Business risks are uncertainties that can impact a company's ability to achieve its strategic objectives.

There are a few key, fundamental points embedded in this definition:

- Risk begins with strategy. A company is in business to achieve a particular strategy, and risks represent the barriers to successfully achieving that strategy. Therefore, companies with different strategies will face different sets of risks.
- Risk does not represent a single point estimate (i.e., the most likely outcome). Rather it represents a range of possible outcomes. Because many different outcomes are possible, the concept of a range is what creates uncertainty when understanding and evaluating risks.
- Risk encompasses both opportunities and threats. Most people focus only on the downside of risk, that is, a hazard or negative outcome that needs to be mitigated or eliminated. While many risks do in fact present a threat, failure to exploit an opportunity or competitive advantage can be a significant risk as well.

Using this broad definition of business risk, one begins to comprehend the extensive number of risks that businesses face as they try to execute their strategies. This extensiveness can be somewhat overwhelming, which brings greater appreciation for the need to have a process to effectively understand and manage the risks across an organization. This need can be addressed through enterprise risk management.

THE TRANSFORMATION TO ERM

The process of managing risks across an entire organization is referred to as *enterprise risk management*. This process is defined as follows:

Enterprise risk management (ERM) is a structured and disciplined approach to help management understand and manage the uncertainties that can threaten a company's success.

The key points embedded in this definition are:

- Just like business risk, ERM also begins with strategy. Its ultimate focus is on managing the risks that can prevent a company from being successful.
- ERM encompasses the entire organization or enterprise. While the concepts can be applied at lower levels within an organization, the ability to aggregate and manage risks enterprise-wide is part of the value provided by ERM.
- Risks represent the uncertainties that can threaten a company's success. Therefore, understanding and identifying risks is an important part of ERM.
- A structured and disciplined approach is necessary to ensure that all risks are identified, and that all of the company's primary risks are effectively managed. An ad hoc or informal approach may fall short of comprehensively identifying all business risks, or may result in resources being devoted to risks that are not primary and, therefore, are not appropriate for devoting valuable risk management resources.

ERM is not a radical, new management approach, but rather a transformation from other management approaches. It provides stakeholders, board members, and senior management with greater confidence that risks are comprehensively identified and understood, and that valuable resources will be devoted to those areas where they are most needed. A structured and disciplined approach goes beyond just managing by instinct; it provides a process that enables individuals across the organization to manage risks in a consistent manner.

The Underlying Impetus

Risk management concepts are not new to the business world. Several industries, the most prominent one being financial services, have developed well documented and tested risk management approaches surrounding key risks in those industries.

However, understanding and managing well-known key business risks may not be enough in today's business environment. As cited in *Enterprise Risk Management: Implementing New Solutions*, Mercer Management Consulting conducted a study of the 100 largest one-month drops in shareholder value in the Fortune 1000 between 1993 and 1998. This study noted:

- Ten percent of the Fortune 1000 companies suffered a loss in shareholder value exceeding 25% within one month of announcing a surprise.
- Two years later, *none* of those companies had fully recovered the value lost, when compared to the S&P 500 during that period.

- Only 6% of the surprises related to financial and hazard risks. The low number of incidents in these two areas reflects the sophistication of financial and hazard risk management techniques that are widely available and in place in most companies.
- The remaining 94% of the surprises related to strategic and operational risks. This reflects the general lack of sophisticated risk management focus in these areas. However, more than two-thirds of these surprises could have been mitigated through available risk management tools and techniques.

This and other studies published in the mid- to late 1990s began to tell a story of companies that suffered severely when certain risks arose, or achieved great success through the deployment of effective ERM techniques. As a result, formalized ERM techniques began to evolve among forward-thinking companies.

More recently, there have been many business failures and significant losses in market value in the post-Enron, bear stock market. Some of the events leading to those losses include financial reporting irregularities, credit rating downgrades, and earnings shortfalls. Companies that effectively identify, assess, and manage the underlying risks driving these events stand the best chance of recovering market value when compared with companies that do not effectively employ these ERM techniques.

Fundamental ERM Techniques

No single ERM approach has been promulgated and adopted by companies throughout the world. Rather, ERM approaches have evolved within companies from many different industries. However, in a landmark research study conducted by the Economist Intelligence Unit in 1994, entitled *Managing Business Risk: An Integrated Approach*, three essential elements were identified for developing an integrated approach to managing business risks:

1. **Develop a common business risk language.** It is important for all employees to speak the same language when discussing and managing risks to ensure effective and quick communications across the organization.
2. **Develop an effective organizational control structure.** Because companies operate in dynamic, changing environments, it is important to ensure that the organization has a control structure that promotes the early identification, assessment, and management of key risks.
3. **Create a process view: Business process control.** In order to operationalize risk management throughout an organization (that is, make it part of all management activities), risk management must be embedded within all key processes to ensure that risks can be managed effectively.