Enterprise Risk Management
and COSO

A Guide for Directors, Executives,
and Practitioners

HARRY CENDROWSKI
WILLIAM C. MAIR

John Wiley & Sons, Inc.
Contents

About the Contributors xi
Acknowledgments xv
Preface xvii

SECTION I ORGANIZATIONAL RISK MANAGEMENT 1
Organizational Risk Management 2
The Risk Assessment Process 4
Risk Management at the Board Level 5
The Importance of Proper Risk Management 6
Preview of Section I 7

CHAPTER 1 An Introduction to Risk 9
Definition of Risk 9
The Risk Management Strategy 11
The Scope of a Risk Management Engagement 13
Influences in Risk Assessments 14
Summary 16

CHAPTER 2 Key Tenets of Enterprise Risk Management 17
Organizational Culture and Risk Management 18
Emphasizing Accountability 20
Planning for Black Swans 21
Benefits of a Risk Management–Focused Culture 22
Issues in Managing Risk 27
Summary 37
Notes 37
Contents

Summary 97
Notes 97

CHAPTER 6  Other Control Frameworks 99
Professional Standards for CPAs 99
Other Control Principles and Frameworks 103
Insurance Model Audit Law 110
Summary 111
Notes 111

CHAPTER 7  Qualitative Control Concepts 113
What Is Control? 114
What Can Go Wrong: Causes of Exposures 116
Effects of Computers and Automation on Problems 117
The System of Internal Control 118
Control Assessment 120
Understand the System 121
List the Potential Problems 122
Estimate the Inherent Risk of Each Problem 123
Segregate Controls and Fundamental Activities 123
Classify the Controls 124
Functions of Controls 129
Assess the Effectiveness of Controls 139
Assess the Adequacy of Control Over Each Problem 141
Appraise Adverse Resulting Consequences 142
The Control Evaluation Matrix 143
How Much Control Is Enough or Too Much? 148
Summary 149
Notes 149

CHAPTER 8  Quantitative Control Relationships 151
Systems Control Functions 152
Preliminary Risk and Potential Incidents 159
Anyone Can Build a Model . . . 173
Precision of Results 175
Sensitivity of Results 176
Summary 177
Notes 177
CHAPTER 9  Excel Applications  179
The Environment  179
Applications of Excel Worksheets  180
What Can Go Wrong with Excel Applications?  181
Excel Controls  185
An Excel Model  187
Summary  188
Note  189

CHAPTER 10  Interdependent Systems  191
Interdependencies  191
Hierarchy of Systems  198
Summary  201

CHAPTER 11  Documentation  203
Documentation Objectives  203
Elements of Control Documentation  204
Common Documentation Formats  206
Documentation Tools  211
Notes  217

CHAPTER 12  The Process for Assessing Internal Control  219
How Does This Fit into Coso  220
System Assessments Steps  220
Summary  237
Note  237

CHAPTER 13  Monitoring Internal Controls  239
COSO Monitoring Guidance  239
The Control Environment  242
Potential Monitoring Problems  243
 Controls Over Controls to Assure Effective Monitoring  248
Assessing the Monitoring Function Under COSO  255
Summary  255
Note  256
Contents

CHAPTER 14  Accounting Policies and Procedures  257
            The Accounting Environment  257
            Conversion from GAAP to IFRS  259
            What Can Go Wrong with Accounting Policies
            and Procedures?  262
            Reliance on Application Systems  265
            Controls Over Accounting Policy Selection and
            Application  266
            Notes  272

CHAPTER 15  Business Process Applications  273
            Application Components, Structure, and Architecture  273
            What Can Go Wrong with Applications?  276
            Typical Application Controls  277
            An Application Assessment Model  280
            Summary  283

CHAPTER 16  General and Infrastructure Systems  285
            The Environment  285
            CobiT for Control of IT  285
            What Can Go Wrong with General Systems?  287
            Controls over General Systems  290
            Infrastructure Model  291
            Summary  293

CHAPTER 17  Trusted System Providers  295
            The Environment  295
            How Much to Trust Trusted Systems?  296
            Provider Problems  297
            Internal Controls over Trusted Systems  298
            A Trusted Provider Assessment Model  301
            Summary  302

CHAPTER 18  Reporting on Internal Control  303
            The Environment  303
            Perception of Risk  304
<table>
<thead>
<tr>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Results of Modeling</td>
</tr>
<tr>
<td>Summary</td>
</tr>
<tr>
<td>Notes</td>
</tr>
<tr>
<td><strong>CHAPTER 19</strong></td>
</tr>
<tr>
<td>Summary Description of the Assessment Model</td>
</tr>
<tr>
<td>The Basic Modeling Concept</td>
</tr>
<tr>
<td>Questions for an Assessment Review</td>
</tr>
<tr>
<td>Summary</td>
</tr>
<tr>
<td><strong>Glossary</strong></td>
</tr>
<tr>
<td><strong>Appendix: Internal Control Sections of the Sarbanes-Oxley Act</strong></td>
</tr>
<tr>
<td>Sec. 301. Public Company Audit Committees</td>
</tr>
<tr>
<td>Section 302</td>
</tr>
<tr>
<td>Sec 404. Management Assessment of Internal Controls</td>
</tr>
<tr>
<td>Sec. 407. Disclosure Of Audit Committee Financial Expert</td>
</tr>
<tr>
<td><strong>Index</strong></td>
</tr>
</tbody>
</table>
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 also 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 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.