Additional Praises for Governance, Risk, and Compliance Handbook

“In just a few short years, GRC has quickly risen to become a top boardroom and management priority at leading organizations around the world. And with business and regulatory environments becoming increasingly complex, the corporate-wide focus on GRC shows no sign of slowing down. The GRC Handbook is a comprehensive guide to the key strategies, tools and best practices that can help companies build and manage a proactive, integrated, cross-enterprise GRC strategy. For companies large or small, across all industries and geographies–this thorough study approaches GRC from multiple perspectives and is a must-have resource for any manager tasked with aligning GRC activities to drive business performance and competitive advantage.”

—Jim Hagemann Snabe, Corporate Officer SAP Group, Member of the Executive Council

“This book provides insightful views of the challenges and lessons learned from the implementation of International and US standards in Latin America. Highly recommended for anyone interested in Global Compliance.”

—Zenon A. Biagosch, Certified Fraud Examiner, Member of the Board of Directors, Central Bank of Argentina

“The GRC Handbook is a must-read for all those involved in Global Compliance. The new international landscape and the interaction among laws, regulations, and professional standards are comprehensively covered in this book.”


“Dr. Anthony Tarantino has produced a classic reference volume on governance, risk, and compliance. His book provides a comprehensive overview of current practices across the globe. This book is a must for practitioners, risk managers, and senior executives.”

—June Yee Felix, General Manager, General Manager Global Banking Solutions and Strategy, IBM

“Today, global level governance, risk management, and compliance are strong management tool for successful international companies. Leading players in this area gain their competitive advantage by penetrating their management style to their every regional entity. Governance, Risk, and Compliance Handbook is unique and comprehensive because it not only covers key GRC topics but also explains governance by industry and by nation. The text will be a good guide for executives and managers who involve in global management.”

—Satoshi Arai, Leader of Risk, Compliance & Security, Japan Management Director, BearingPoint Co., Ltd.
BECOME A SUBSCRIBER!

Did you purchase this product from a bookstore?

If you did, it's important for you to become a subscriber. John Wiley & Sons, Inc. may publish, on a periodic basis, supplements and new editions to reflect the latest changes in the subject matter that you need to know in order to stay competitive in this ever-changing industry. By contacting the Wiley office nearest you, you'll receive any current update at no additional charge. In addition, you'll receive future updates and revised or related volumes on a 30-day examination review.

If you purchased this product directly from John Wiley & Sons, Inc., we have already recorded your subscription for this update service.

To become a subscriber, please call 1-800-225-5945 or send your name, company name (if applicable), address, and the title of the product to:

mailing address: Supplement Department
John Wiley & Sons, Inc.
One Wiley Drive
Somerset, NJ 08875

e-mail: subscriber@wiley.com
fax: 1-732-302-2300

For customers outside the United States, please contact the Wiley office nearest you:

Professional & Reference Division
John Wiley & Sons Canada, Ltd.
22 Worcester Road
Rexdale, Ontario M9W 1L1
CANADA
(416) 675-3580
Phone: 1-800-567-4797
Fax: 1-800-565-6802
canada@wiley.com

PRT Division
Jacaranda Wiley Ltd.
P.O. Box 174
North Ryde, NSW 2113
AUSTRALIA
Phone: (02) 905-1100
Fax: (02) 905-1597
headoffice@jacwiley.com.au

John Wiley & Sons, Ltd.
Baffins Lane
Chichester
West Sussex, PO19 1UD
ENGLAND
Phone: (44) 1243 779777
Fax: (44) 1243 776838
cs-books@wiley.co.uk

John Wiley & Sons (SEA) Pte. Ltd.
2 Clementi Loop #02-01
SINGAPORE 129809
Phone: 65 463 2400
Fax: 65 463 4605; 65 463 4604
wiley@singnet.com.sg
GOVERNANCE, RISK, AND COMPLIANCE HANDBOOK

TECHNOLOGY, FINANCE, ENVIRONMENTAL, AND INTERNATIONAL GUIDANCE AND BEST PRACTICES

Edited By

ANTHONY TARANTINO, PhD

WILEY

JOHN WILEY & SONS, INC.
To my Beloved Xuelian

“Everyone must submit himself to the governing authorities, for there is no authority except that which God has established. The authorities that exist have been established by God. Consequently, He who rebels against the authority is rebelling against what God has instituted, and those who do so will bring judgment on themselves. For rulers hold no terror for those who do right, but for those who do wrong. Do you want to be free from fear of the one in authority? Then do what is right and he will commend you. For he is God’s servant to do you good. But if you do wrong, be afraid, for he does not bear the sword for nothing. He is god’s servant, an agent of wrath to bring punishment on the wrongdoer. Therefore, it is necessary to submit to the authorities, not only because of possible punishment but also because of conscience. This is also why you pay taxes, for the authorities are god’s servants, who give their full time to governing. Give everyone what you owe him: if you owe taxes, pay taxes; if revenue, then revenue; if respect, then respect; if honor, then honor.

Romans 13: 1-7: Submission to the Authorities

The Mandate of Heaven is conditioned on virtuous rule, is not perpetual or automatic and depends on good governance worthy of a virtuous sovereign. The Mandate of Heaven can be lost through the immoral behavior of the ruler, or failings in his responsibility for the welfare of the people, in which case Heaven will grant another, more moral individual a new mandate to found a new dynasty. Loyalty will inspire loyalty. Betrayal will beget betrayal. A king unworthy of his subjects will be rejected by them. Such is the will of Heaven.

Mencius (Meng-Tze), 孟子, Book of Mencius, (371-288 B.C.)
# CONTENTS

Preface xxxiii  
Acknowledgments xxxv  
About the Contributors xxxvii  

## CHAPTER 1  INTRODUCTION  
1.1 Act Locally, Impact Globally 1  
1.2 Governance 2  
1.3 Risk 15  
1.4 Compliance and Internal Controls 21  
1.5 GRC and Globalization 25  
1.6 Growth of Global Trade 30  
1.7 Simple Suggestions to Improve Governance, Risk Management, and Compliance (GRC) 30  
1.8 Why Read This Book: The Case for Good GRC 35  
1.9 Organization of the Handbook 36  

## PART 1  Corporate Governance 39  

### CHAPTER 2  A RISK-BASED APPROACH TO ASSESS INTERNAL CONTROL OVER FINANCIAL REPORTING (ICFR) 41  
2.1 A Risk-Based Approach to Assessing ICFR 42  
2.2 Determine Key Stakeholders 42  
2.3 Establish the Risk Management Context 44  
2.4 Risk Rating and Risk Identification 47  
2.5 Analyze and Evaluate Risks 51  
2.6 Treat/Mitigate Risks 52  
2.7 Identify, Assess, and Report on Residual Risk Status 62  
2.8 Concluding Remarks 64  

### CHAPTER 3  COSO—IS IT FIT FOR PURPOSE? 65  
3.1 The Roots of COSO 66
3.2 COSO the Committee and COSO the 1992 Integrated Control Framework: Have They Stood the Test of Time? 69
3.3 Actual Market Acceptance of the COSO 1992 Framework Prior to SOX 70
3.4 Expectations of COSO Escalate Overnight 71
3.5 Is COSO 1992 Free from Bias? 72
3.6 Does COSO 1992 Permit Consistent Quantitative/Qualitative Measurement? 73
3.7 Is COSO 1992 Sufficiently Complete So That Relevant Factors Are Not Omitted? 73
3.8 Is COSO 1992 Relevant to an Analysis of Controls over Financial Reporting? 74
3.9 COSO: Looking Forward 75

CHAPTER 4 Time to Rethink the Corporate Tax 77
4.1 Q&A with Mihir Desai 77
4.2 About Faculty in This Article 81

CHAPTER 5 The Role of Internal Audit 83
5.1 Introduction 83
5.2 Internal Auditors’ Role Throughout History 83
5.3 The Role Transformed 86
5.4 Beyond Assurance: Advisory Services 87
5.5 Achieving the Greatest Impact 89
5.6 The Bright Outlook of Internal Auditing 92

CHAPTER 6 Outsourced Processes: Risk and Resolution 95
6.1 A Matter of Risk 95
6.2 A Matter of Responsibility 96
6.3 Outsourced Risk Management 97
6.4 SAS 70 Criticisms 99
6.5 SAS 70 Alternatives 100
6.6 Summary 100

CHAPTER 7 The Last Mile of Finance 103
7.1 The Last Mile of Finance 103
CONTENTS xi

7.2 Regaining Control 104
7.3 Where Everything Comes Together 105
7.4 The Path to an Optimum Close 107
7.5 A Return to Good Finance 109

CHAPTER 8 U.S. STOCK OPTION BACKDATING SCANDALS 111
8.1 Introduction 111
8.2 The Pros and Cons of Stock Options 113
8.3 The American Scandals 113
8.4 Why Stock Options Should Be Avoided 116
8.5 Suggestions in Managing Options for Those Who Must Retain Them 116
8.6 How the United States Got into Such a Mess 118

CHAPTER 9 FRAUD AND CORRUPTION 121
9.1 What Are Fraud and Corruption? Historical Background from Ethics 121
9.2 Consequences of Fraud and Corruption for an Individual, Business, and Community 123
9.3 Principal-Agent Problem with Practices and Procedures for Managing Fraud and Corruption 125
9.4 Best Practice Guidelines for Detection Methods, Including Checking of Background and References 126
9.5 Data Mining for Detection of Fraud and Corruption 126
9.6 Corporate Governance, Compliance Issues, and Knowing Your Employees and Clients 127
9.7 Enforcement, Incentive Schemes, and Market Solutions Preventing Fraud and Corruption 130

CHAPTER 10 WHY FIGHTING CORRUPTION REMAINS A LOSING BATTLE 133
10.1 Introduction: The Fight against Corruption Requires a Deeper Understanding of the Underlying Malaise 133
10.2 Corruption and Governance: Fundamental Concepts and Concerns 134
10.3 What Drives Corruption? 136
10.4 Conclusions: Don’t Use the “C” Word 145

PART 2  IT Governance  153

CHAPTER 11 IT GOVERNANCE OVERVIEW  155
11.1 Governance Background  155
11.2 Information Economy, Intellectual Capital  157
11.3 Competitiveness  158
11.4 IT Service Delivery  158
11.5 Governance Convergence  159
11.6 Strategic and Operational Risk Management  160
11.7 Regulatory Compliance  161
11.8 Information Risk  162
11.9 Strategic System Deployment and Project Governance  162
11.10 IT Governance Frameworks and Tools  163
11.11 Frameworks  164
11.12 AS 8015-2005  164
11.13 IT Governance—The Implementation Challenge  165
11.14 Benefits of an IT Governance Framework  165

CHAPTER 12 ISO 27001 AND ISO 17799  169
12.1 ISO 27001 and ISO 17799—The Information Security Standards  169
12.2 ISO 17799 versus ISO 27001  172
12.3 Conclusion  178
12.4 Essential Further Reading  179

CHAPTER 13 COBIT  181
13.1 Background  181
13.2 History  182
13.3 COBIT CUBE  184
13.4 Linking Business Goals to IT Goals  187
| 13.5 | How Will COBIT 4.x Impact/Benefit Users? | 188 |
| 13.6 | Conclusion | 188 |

## PART 3 Operational Risk

### CHAPTER 14 OPERATIONAL RISK MANAGEMENT (ORM) BEST PRACTICES

14.1 Introduction | 193 |
14.2 Defining Operational Risk | 195 |
14.3 Tone at the Top and Corporate Culture | 195 |
14.4 Documentation | 196 |
14.5 Policies and Procedures | 196 |
14.6 Independent Audit | 196 |
14.7 Management Oversight | 197 |

### CHAPTER 15 THE USE OF SIX SIGMA IN OPERATIONAL RISK AND REGULATORY COMPLIANCE: REDUCTION IN VARIABILITY

15.1 What Is Six Sigma? | 200 |
15.2 The Six Sigma Methodology | 201 |
15.3 The Hard Tools of Six Sigma | 206 |
15.4 The Soft Tools of Six Sigma | 211 |
15.5 Conclusion | 212 |

### CHAPTER 16 OPERATIONAL RISK MANAGEMENT USING QUANTITATIVE METHODS

16.1 Introduction | 213 |
16.2 Defining Operational Risk | 215 |
16.3 Defining Quantitative Analysis (Quantitative Methods) | 216 |
16.4 Advantages and Disadvantages of Using Quantitative Methods | 217 |
16.5 Operational Risk Assessment and Management—Essential Components | 217 |
16.6 Quantify Operational Risk | 226 |
16.7 Monitor and Control Operational Risk | 229 |
16.8 Change Management | 229 |