Governance, Risk Management, and Compliance

It Can’t Happen to Us—Avoiding Corporate Disaster While Driving Success

Richard M. Steinberg

Foreword by Arthur Levitt
Additional praise for

**Governance, Risk Management, and Compliance**

*It Can’t Happen to Us—Avoiding Corporate Disaster While Driving Success*

“In this complex and perilous global marketplace, it is vital that corporate leaders—senior officers and board members—put the highest premium on being smart about managing risk. Richard Steinberg has written a superb resource not only for strengthening your governance, risk management, and compliance practices but also ensuring they lead to competitive advantage.”

—James Kristie, Editor, *Directors & Boards*

“A practical and commonsense approach to corporate governance from someone who knows the subject well!”

—Richard Koppes, former Deputy Executive Officer and General Counsel of CalPERS, founder of the National Association of Public Pension Attorneys, and board member of the National Association of Corporate Directors

“This compelling work by Rick Steinberg enables even experienced senior managers and board members to fully appreciate how governance can and should work. Filled with critical analyses of how major companies have stumbled or failed, with clear lessons to be learned of what needs to go right, this book should be required reading for all of us striving to see our businesses thrive and grow shareholder value.”

—Scott Eston, former Chief Operating Officer, GMO
Governance, Risk Management, and Compliance
Governance, Risk Management, and Compliance

It Can’t Happen to Us—Avoiding Corporate Disaster While Driving Success

RICHARD M. STEINBERG
This book is dedicated to my wonderful wife, Lana, without whose love and support it never would have been written.
## Contents

Foreword  xiii  
Preface  xix  
Acknowledgments  xxiii  

**Chapter 1: What Is GRC, and Why Does It Matter?**  1  
What Is GRC?  2  
Why GRC Matters  3  

**Chapter 2: Culture, the Critical Driver**  5  
What Is Culture?  5  
More Cultural Failures  6  
Companies That Got It Right  8  
Being Legal, Honest, Candid, and . . .  10  
Integrity versus Spin  13  
Speaking the Same Language  16  

**Chapter 3: Cost-Effective Compliance Programs**  21  
The Back-Breaking Costs  22  
Beyond the Direct Costs  24  
Major Mistakes at Platinum-Branded Companies  24  
How Companies Got Where They Are  30  
Keys to Getting It Right  31  
The Compliance Office  36  
Making It Happen  38  
The Rewards  39
Chapter 9: Control over Operational Performance

IT Controls 134
Société Générale 135
Washington Mutual 139
Countrywide Financial Corporation 143
The Foreclosure Fiasco 144

Chapter 10: Boards of Directors’ Focus

A Focus on the Rules 155
Truly Effective Boards 156
A Public Watchdog? 158
Societal Responsibility 160
Potential Pitfalls 163

Chapter 11: Overseeing Strategy and Risk Management

Strategy 169
Risk Management 173

Chapter 12: CEO Compensation, Succession Planning, and Crisis Management

CEO Compensation 185
Succession Planning 192
Crisis Management 196

Chapter 13: Performance Measurement and Reporting

Performance Measures 201
Financial Reporting 205

Chapter 14: Building an Effective Board

Looking Objectively 220
A Shift in Direction 221
Building a Better Board 223
Board Assessments 226
Bottom Line 230
Chapter 15: Avoiding Board Pitfalls

- Following the Herd
- Obtaining Critical Information
- A Leaky HP Board
- Another Leak—What Was He Thinking?

Chapter 16: Where the Power Lies

- A Tug of War
- Shareholder Activism
- Recent Achievements
- Dodd-Frank’s Proxy Access
- Where to Draw the Line
- Finding the Right Balance
- Where We Need to Evolve

Chapter 17: Structural Issues at the Board

- Combined versus Separate Chairman and CEO
- Empowering CEOs in a Shifting Landscape
- Director Compensation

Chapter 18: Looking to the Future

- New Models for Board Governance
- A Healthy Governance Environment
- Boards’ Perspectives on Risk
- Grasping the Holy Grail of Governance
- What the Future Holds

About the Author

Index
In the aftermath of the worst economic and financial crisis in the United States in decades, policymakers, journalists, investor advocates, and others have been hard at work trying to identify those responsible. Commissions have met and studies have been undertaken, and people are beginning to reach their conclusions. But at the very core of this crisis was not a single set of actors. The problems stem significantly and systematically from the failure of governance, oversight, and risk management at the corporate, legislative, and regulatory levels.

Those in position to imagine, identify, and reduce the possibilities of failure simply did not do their jobs. As Richard Steinberg makes clear in these pages, the price of inattention or inaction by managers, regulators, and board members could be measured not in the hundreds of millions of dollars, but in the hundreds of billions of dollars. He explains how reputations and corporations were shattered in a matter of weeks and months, because individuals and institutions had no means of checking and correcting their market assumptions and their culture of risk-taking. In short, not enough people were asking: “What could go wrong?”

This failure in governance pains me deeply, primarily because as a regulator throughout the 1990s I was able to see many of these same failures play out once before in corporate America and our regulatory infrastructure. Many of the biggest changes in corporate governance were launched just after the Enron, WorldCom, and other major scandals of the early 2000s. And the resulting reforms, especially Sarbanes-Oxley, have had deep and lasting impacts.

In the immediate aftermath of those scandals, we saw a revolution in thinking about governance. Most boards are now majority independent—and key committees are now entirely independent, except at some controlled companies. Most companies have a lead independent director and/or a separate chairman. Boards meet more frequently—both as a whole and in executive session without the CEO—and are under significant scrutiny by shareholders. What’s more, SEC rules have enabled shareholders to interact with each other...