



WILEY CORPORATE F&A

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



WILEY

John Wiley & Sons, Inc.

Copyright © 2011 by Steinberg Governance Advisors, Inc. All rights reserved.

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

Published simultaneously in Canada.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise, except as permitted under Section 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 646-8600, or on the Web at www.copyright.com. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at <http://www.wiley.com/go/permissions>.

Limit of Liability/Disclaimer of Warranty: While the publisher and author have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the publisher nor author shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

Some content in this book was originally published in columns by the author in Compliance Week, an information service on governance, risk and compliance. For more information, visit www.complianceweek.com or call (888) 519-9200.

For general information on our other products and services or for technical support, please contact our Customer Care Department within the United States at (800) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books. For more information about Wiley products, visit our web site at www.wiley.com.

Library of Congress Cataloging-in-Publication Data:

Steinberg, Richard.

Governance, risk management, and compliance : it can't happen to us—avoiding corporate disaster while driving success / Richard Steinberg.

p. cm.

Includes index.

ISBN 978-1-118-02430-0 (hardback); ISBN 978-1-118-10255-8 (ebk);
ISBN 978-1-118-10256-5 (ebk); ISBN 978-1-118-10257-2 (ebk)

1. Corporate governance. 2. Risk management. 3. Compliance.
4. Business planning. I. Title.

HD2741.S7636 2011

658'—dc22

2011012036

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

*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 4: Ethics Programs: Another Foundational Block	41
Tone at the Top	42
Problems at Daimler	42
Elements of an Ethics Program	43
Setting the Tone at the Top: Hewlett-Packard	51
 Chapter 5: Risk Management and the Financial System's Near Meltdown	 59
What Went So Terribly Wrong	59
The Regulatory System	63
Merrill Lynch	65
Where Were the Boards?	68
Did CEOs See It Coming?	70
 Chapter 6: What Is Risk Management About?	 75
Risk	76
Risk Management	79
Enterprise Risk Management	80
Is It Really Worth the Effort?	85
ERM Application Techniques	88
Key Risk Indicators	91
BP	92
 Chapter 7: Implementing ERM	 99
Drivers for ERM	99
Pitfalls	102
Effective Implementation	106
Roles and Responsibilities	114
 Chapter 8: Does Internal Control Really Matter?	 119
Impact of SOX 404 on Financial Reporting	122
Responsibility for SOX 404	124
Other Relevant SOX Provisions	126
Do Effective Financial Reporting Controls Really Prevent	
Fraudulent Financial Reporting?	127
Real Life in the C-Suite	130

Chapter 9: Control over Operational Performance	133
IT Controls	134
Société Générale	135
Washington Mutual	139
Countrywide Financial Corporation	143
The Foreclosure Fiasco	144
 Chapter 10: Boards of Directors' Focus	 153
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	 169
Strategy	169
Risk Management	173
 Chapter 12: CEO Compensation, Succession Planning, and Crisis Management	 185
CEO Compensation	185
Succession Planning	192
Crisis Management	196
 Chapter 13: Performance Measurement and Reporting	 201
Performance Measures	201
Financial Reporting	205
 Chapter 14: Building an Effective Board	 219
Looking Objectively	220
A Shift in Direction	221
Building a Better Board	223
Board Assessments	226
Bottom Line	230

Chapter 15: Avoiding Board Pitfalls	231
Following the Herd	231
Obtaining Critical Information	238
A Leaky HP Board	245
Another Leak—What Was He Thinking?	249
Chapter 16: Where the Power Lies	251
A Tug of War	252
Shareholder Activism	252
Recent Achievements	253
Dodd-Frank's Proxy Access	256
Where to Draw the Line	261
Finding the Right Balance	262
Where We Need to Evolve	264
Chapter 17: Structural Issues at the Board	265
Combined versus Separate Chairman and CEO	265
Empowering CEOs in a Shifting Landscape	271
Director Compensation	274
Chapter 18: Looking to the Future	281
New Models for Board Governance	281
A Healthy Governance Environment	285
Boards' Perspectives on Risk	289
Grasping the Holy Grail of Governance	290
What the Future Holds	293
About the Author	299
Index	301

Foreword

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