

Sarbanes- Oxley

FOR

DUMMIES®

2ND EDITION

by Jill Gilbert Welytok, JD, CPA



WILEY

Wiley Publishing, Inc.

*Sarbanes-
Oxley*

FOR

DUMMIES[®]

2ND EDITION

Sarbanes- Oxley

FOR

DUMMIES[®]

2ND EDITION

by Jill Gilbert Welytok, JD, CPA



WILEY

Wiley Publishing, Inc.

Sarbanes-Oxley For Dummies®, 2nd Edition

Published by
Wiley Publishing, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

Copyright © 2008 by Wiley Publishing, Inc., Indianapolis, Indiana

Published by Wiley Publishing, Inc., Indianapolis, Indiana

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 Sections 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, 222 Rosewood Drive, Danvers, MA 01923, 978-750-8400, fax 978-646-8600. Requests to the Publisher for permission should be addressed to the Legal Department, Wiley Publishing, Inc., 10475 Crosspoint Blvd., Indianapolis, IN 46256, 317-572-3447, fax 317-572-4355, or online at <http://www.wiley.com/go/permissions>.

Trademarks: Wiley, the Wiley Publishing logo, For Dummies, the Dummies Man logo, A Reference for the Rest of Us!, The Dummies Way, Dummies Daily, The Fun and Easy Way, Dummies.com and related trade dress are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates in the United States and other countries, and may not be used without written permission. All other trademarks are the property of their respective owners. Wiley Publishing, Inc., is not associated with any product or vendor mentioned in this book.

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THE PUBLISHER AND THE AUTHOR MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES OR PROMOTIONAL MATERIALS. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY SITUATION. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL SERVICES. IF PROFESSIONAL ASSISTANCE IS REQUIRED, THE SERVICES OF A COMPETENT PROFESSIONAL PERSON SHOULD BE SOUGHT. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. THE FACT THAT AN ORGANIZATION OR WEBSITE IS REFERRED TO IN THIS WORK AS A CITATION AND/OR A POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE AUTHOR OR THE PUBLISHER ENDORSES THE INFORMATION THE ORGANIZATION OR WEBSITE MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. FURTHER, READERS SHOULD BE AWARE THAT INTERNET WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ.

For general information on our other products and services, please contact our Customer Care Department within the U.S. at 800-762-2974, outside the U.S. at 317-572-3993, or fax 317-572-4002.

For technical support, please visit www.wiley.com/techsupport.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.

Library of Congress Control Number: 2008920765

ISBN: 978-0-470-22313-0

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1



About the Author

Jill Gilbert Welytok, JD, CPA, LLM, practices in the areas of corporate, non-profit law, and intellectual property. She is the founder of Absolute Technology Law Group, LLC (www.abtechlaw.com). She went to law school at DePaul University in Chicago, where she was on the Law Review, and she picked up a Masters Degree in Computer Science from Marquette University in Wisconsin, where she now lives. Ms. Welytok also has an LLM in Taxation from DePaul. She was formerly a tax consultant with the predecessor firm to Ernst & Young. She frequently speaks on nonprofit, corporate governance, and taxation issues and will probably come speak to your company or organization if you invite her. You may e-mail her with questions you have about Sarbanes-Oxley or anything else in this book at jwelytok@abtechlaw.com. You can find updates to this book and ongoing information about SOX developments at the author's Web site, located at www.abtechlaw.com.

Dedication

To Dan.

Author's Acknowledgments

Several exceptional professionals (whom I call The SOX SWAT Team) contributed their time and expertise reviewing and making technical edits to this book. Feel free to e-mail or call them with questions you may have about Sarbanes-Oxley that weren't answered in this book.

Amy R. Seibel. Amy is an attorney and a CPA with Absolute Technology Law Group, LLC. Amy is an AV- rated attorney (highest rating available for lawyers) with more than 25 years of experience in legal, business, tax, and financial matters. She has practical experience as well, having previously served as CEO/CFO for two separate manufacturing businesses. More recently, she assisted several large public companies in the documentation, testing, and remediation phases of their SOX internal controls compliance initiatives. She also served as a technical editor for *Nonprofit Law & Governance For Dummies*. She is past president of the Association for Women Lawyers and past chairman of the Wisconsin and Milwaukee Bar Association Tax Sections.

Richard Kranitz, JD — Kranitz & Philipp. Rich has been an attorney in private practice since 1970, emphasizing securities, banking, and business law. He has served as venture capital consultant to, and director of, various private companies and a number of professional, civic, and charitable organizations.

Ronald Kral, CPA, CMA — Candela Solutions, LLC. Ron knows auditing and consulting well, having assisted more than 200 clients as a Principal Consultant at PricewaterhouseCoopers and Managing Director of a statewide CPA firm, where he worked extensively with Ernst & Young. Ron is a nationally recognized speaker on governance, business ethics, internal controls, and the Sarbanes-Oxley Act of 2002, including the COSO and COBIT frameworks, NYSE and NASDAQ requirements, PCAOB standards, and SEC regulations. Ron is also a Director of Financial Executives International's Milwaukee Chapter. He can be reached at rkral@candelasolutions.com.

Anna Klement. Anna has completed coursework in computer engineering at the Milwaukee School of Engineering and also has a journalism degree from the University of Wisconsin-Milwaukee. Anna also has three years of experience as an IBM applications developer at a major Milwaukee-based food manufacturing firm, along with various freelance projects including Web and graphic design and technology consulting.

Daniel S. Welytok, JD, LL.M. — Whyte Hirschboeck Dudek S.C. Dan is a partner in the business practice group of Whyte Hirschboeck Dudek S.C., where he concentrates in the areas of taxation and business law. Dan advises clients on strategic planning, federal and state tax issues, transactional matters, and employee benefits. He represents clients before the IRS and state taxing authorities concerning audits, tax controversies, and offers in compromise. He has served in various leadership roles in the American Bar Association and as Great Lakes Area liaison with the IRS. He can be reached at dsw@whdlaw.com.

Publisher's Acknowledgments

We're proud of this book; please send us your comments through our Dummies online registration form located at www.dummies.com/register/.

Some of the people who helped bring this book to market include the following:

Acquisitions, Editorial, and Media Development

Project Editor: Natalie Faye Harris
(*Previous Edition: Tim Gallan*)

Acquisitions Editor: Lindsay Lefevere
(*Previous Edition: Kathy Cox*)

Copy Editor: Jessica Smith
(*Previous Edition: Elizabeth Rea*)

Editorial Program Coordinator:
Erin Calligan Mooney

Technical Editor: Amy Seibel

Editorial Manager: Christine Beck

Editorial Assistants: Leeann Harney, David Lutton, Joe Niesen

Cartoons: Rich Tennant (www.the5thwave.com)

Composition Services

Project Coordinator: Kristie Rees

Layout and Graphics: Stacie Brooks,
Alissa D. Ellet, Melissa K. Jester,
Christine Williams

Proofreaders: John Greenough, Todd Lothery,
Toni Settle

Indexer: WordCo Indexing Services

Publishing and Editorial for Consumer Dummies

Diane Graves Steele, Vice President and Publisher, Consumer Dummies

Joyce Pepple, Acquisitions Director, Consumer Dummies

Kristin A. Cocks, Product Development Director, Consumer Dummies

Michael Spring, Vice President and Publisher, Travel

Kelly Regan, Editorial Director, Travel

Publishing for Technology Dummies

Andy Cummings, Vice President and Publisher, Dummies Technology/General User

Composition Services

Gerry Fahey, Vice President of Production Services

Debbie Stailey, Director of Composition Services

Contents at a Glance

<i>Introduction</i>	1
<i>Part I: The Scene Before and After SOX</i>	7
Chapter 1: The SOX Saga	9
Chapter 2: SOX in Sixty Seconds	27
Chapter 3: SOX and Securities Regulations	43
Chapter 4: SOX and Factual Financial Statements	67
Chapter 5: What's New for Non-Accelerated Filers	83
<i>Part II: SOX in the City: Meeting New Standards</i>	89
Chapter 6: A New Audit Ambience	91
Chapter 7: A Board to Audit the Auditors	105
Chapter 8: The Almighty Audit Committee	119
Chapter 9: Building Boards That Can't Be Bought	131
Chapter 10: SOX: Under New Management	143
Chapter 11: More Management Mandates	159
<i>Part III: Scaling Down Section 404</i>	169
Chapter 12: Clearing Up Confusion about Control	171
Chapter 13: Surviving a Section 404 Audit	183
Chapter 14: Taking the Terror Out of Testing	191
<i>Part IV: SOX for Techies</i>	207
Chapter 15: Getting Technical with SOX	209
Chapter 16: Surveying SOX Software	219
Chapter 17: Working with Some Actual SOX Software	233
<i>Part V: To SOX-finity and Beyond</i>	249
Chapter 18: Lawsuits under SOX	251
Chapter 19: The Surprising Scope of SOX	267
<i>Part VI: The Part of Tens</i>	273
Chapter 20: Ten Ways to Avoid Getting Sued or Criminally Prosecuted Under SOX	275
Chapter 21: Ten Tips for an Effective Audit Committee	281

Chapter 22: Ten Smart Management Moves	289
Chapter 23: Ten Things You Can't Ask an Auditor to Do After SOX.....	295
Chapter 24: Top Ten Places to Get Smart about SOX	301
<i>Part VII: Appendixes</i>	307
Appendix A: Selected Sections, Auditing Standard No. 5.....	309
Appendix B: Sample Certifications.....	313
Appendix C: Sample Audit Committee Charter	319
Appendix D: Sample Code of Ethics.....	329
Appendix E: Sample SAS 70 Report.....	337
<i>Index</i>	339

Table of Contents

<i>Introduction</i>	1
About This Book.....	1
Conventions Used in This Book	2
What You're Not to Read.....	2
Foolish Assumptions	3
How This Book Is Organized.....	3
Part I: The Scene Before and After SOX.....	4
Part II: SOX in the City: Meeting New Standards	4
Part III: Scaling Down Section 404	4
Part IV: SOX for Techies.....	4
Part V: To SOX-finity and Beyond.....	4
Part VI: The Part of Tens	5
Part VII: Appendixes.....	5
Icons Used in This Book.....	5
Where to Go from Here.....	6
Feedback, Please	6

Part I: The Scene Before and After SOX..... **7**

Chapter 1: The SOX Saga	9
Plowing Through the Politics of SOX.....	10
Taking advantage of a loophole	10
Not everyone's a SOX fan	11
New ammunition for aggrieved investors	13
Corporate America after SOX	13
Combating Corruption under SOX: Everyone Has a Role	14
Assisting with internal control: The independent audit board	14
Testing the accounting data: Auditors	15
Using the new noisy liability: Lawyers	16
Certifying financial reports: CEOs and CFOs	17
Staying clean voluntarily: Small businesses and nonprofits.....	17
Adhering to procedures: The rank-and-file employees	18
Overseeing corporate policy: New high-paid governance gurus	18
A Summary of SOX: Taking It One Title at a Time.....	18
Title I: Aiming at the audit profession	18
Title II: Ensuring auditor independence	20
Title III: Requiring corporate accountability.....	20
Title IV: Establishing financial disclosures, loans, and ethics codes	21
Title V: Protecting analyst integrity	22
Title VI: Doling out more money and authority.....	22
Title VII: Supporting studies and reports	22

Title VIII: Addressing criminal fraud and whistle-blower provisions	23
Title IX: Setting penalties for white-collar crime	23
Title X: Signing corporate tax returns.....	24
Title XI: Enforcing payment freezes, blacklists, and prison terms.....	24
Some Things SOX Doesn't Say: SOX Myths.....	24
Myth #1: SOX put Jeff Skilling (and other Enron execs) in jail	24
Myth #2: Auditors can't provide tax services.....	25
Myth #3: Internal control means data security	25
Myth #4: The company isn't responsible for functions it outsources.....	26
Myth #5: My company met the deadline for Section 404 first-year compliance. We're home free!	26

Chapter 2: SOX in Sixty Seconds 27

Reestablishing Control after the Scandals.....	28
Enron events everyone initially overlooked.....	28
More tales from the corporate tabloids	32
Four Squeaky Clean SOX Objectives.....	33
How SOX Protects the Investing Public	35
Creating a Public Company Accounting Oversight Board	35
Clamping down on auditors.....	36
Rotating auditors.....	37
Creating committees inside companies	37
Holding management accountable.....	38
Taking back bogus bonuses	38
Banning blackouts.....	38
Ratcheting up reporting	39
Purging company conflicts of interest.....	39
Exercising internal control.....	40
Looking at lawyers	40
Waiting seven years to shred.....	41
Putting bad management behind bars	41
Freezing bonuses.....	41
Blackballing officers and directors	41
Providing whistle-blower protection	42
Rapid Rulemaking Regrets	42

Chapter 3: SOX and Securities Regulations 43

Pre-SOX Securities Laws.....	44
The Securities Act of 1933: Arming investors with information.....	45
The Securities Exchange Act of 1934: Establishing the SEC	46
Other securities laws	49

The Scope of SOX: Securities and Issuers.....49
 What is a “security”?.....50
 Who is an “issuer”?51
 The SOX surprise.....52
 The Post-SOX Paper Trail.....54
 Form 10-K.....55
 Form 10-Q55
 Form 8-K.....56
 Behind the 8-K Ball after SOX56
 Adding new events to the list56
 Shuffling events from the 10-K and 10-Q.....57
 Creating four-day reporting events58
 Providing protection in the safe SOX harbor.....58
 Annual SEC Scrutiny after SOX.....59
 Mandatory review rule59
 Remedies for inaccurate registration materials60
 Why Privately Held Companies Care about SOX60
 Bolstering the bottom line60
 Defending company practices in court62
 Going public after SOX.....62

Chapter 4: SOX and Factual Financial Statements 67

Auditing the Auditors: 2007 Guidance from the SEC68
 SOX’s Recipe for Seeking Out Cooked Books69
 Reviewing what the income statement reveals70
 Examining balance sheet (and off–balance sheet) transactions....72
 Looking for funky footnotes73
 Complying with GAAP and GAAS73
 Finding Financial Information.....75
 The free stuff75
 The fee-based stuff.....76
 Accessing Annual Reports77
 The glossy pictures and the real figures77
 Management’s Discussion and Analysis.....79
 Surfing SEC Filings.....79
 10-K reports.....79
 Other useful forms on EDGAR80

Chapter 5: What’s New for Non-Accelerated Filers 83

A SOX Update for Small Companies.....83
 No relief for non-accelerated filers.....84
 Looking at what the rules require84
 Getting the Auditor’s Opinion85
 A kinder, gentler audit85
 Touting a top-down approach.....86
 Tips for adopting a new “audit-tude”86

Part II: SOX in the City: Meeting New Standards 89**Chapter 6: A New Audit Ambience 91**

How SOX Rocks the Accounting Profession	91
An Example of Audit Failure: Arthur Andersen.....	92
Chronology of a collapse.....	92
A vindicating verdict . . . years later	93
Bridging the GAAP.....	94
SOX as a Substitute for Self-Regulation.....	94
Shifting the role of the AICPA.....	95
Whose turn is it to watch the CPA?.....	97
Is There an Independent Auditor in the House?	97
The importance of audit independence	98
Every auditor's dilemma	99
What SOX Says to CPAs	99
Give the whole team a cooling-off period.....	100
Prohibit services that cause conflicts	100
Get prior permission for potential conflicts	101
Everybody change partners!.....	102
Wait seven years to shred	102
Recognize when auditors are "impaired"	102
Section 404: The Sin Eater Provision	102
CEOs and CFOs signing off	103
CPAs certifying the certifications.....	103

Chapter 7: A Board to Audit the Auditors 105

Taking a New Approach to Audit Oversight	106
The old ad hoc system of accounting oversight	106
Alphabet soup of accounting regulation	107
Primary Purposes of the PCAOB.....	108
Goals of the PCAOB.....	108
The seven statutory duties of the PCAOB	109
Some Practical PCAOB Matters.....	109
Who's on the board?	110
Who pays for the PCAOB?.....	110
PCAOB Rules: Old Meets New	110
Sticking to the ol' standby rules.....	111
Adjusting to some new rules.....	111
Evolving PCAOB Policies and Issues	113
Sanctioning sloppy auditors	113
Keeping an eye on small CPA firms	113
Extending authority internationally.....	114
Communicating with the SEC.....	114
When the PCAOB Doesn't Perform	114
Struggling for Standards.....	115
Adapting to Auditing Standard No. 2	115
Implementing Auditing Standard No. 5.....	116

Chapter 8: The Almighty Audit Committee	119
Deliver or Delist: Rules of the Stock Exchanges.....	119
From the Audit Committee Annals.....	121
Mr. Leavitt's Blue Ribbon panel.....	121
Enron impetus.....	121
The quest for consistent committee rules	121
Starting with a Charter	122
The Audit Committee Interface.....	122
Some Stricter NYSE Rules	123
Membership Requirements	124
A few independent members	124
Figure in a financial expert.....	125
Day-to-Day Committee Responsibilities	125
Monitoring events and policing policies	126
Interfacing with the auditors	126
Preapproving nonaudit services	127
Handling complaints	128
Receiving CEO and CFO certifications.....	128
Monitoring conflicts and cooling-off periods	129
Ferretting out improper influence	129
Rotating the audit partners.....	129
Engaging advisors	130
Providing recognition in annual reports	130
Chapter 9: Building Boards That Can't Be Bought	131
Some Background about Boards.....	132
What does a director do?	132
Looking at some bad, bad boards	133
In Search of Independent Directors	134
No relationships with related companies	135
Three-year look-back period.....	136
Prohibited payments.....	136
Family ties	136
Mandatory meetings	137
Forming Committees for Nominating Directors	137
NYSE nominating procedures	138
NASDAQ nominating rules	138
Regulating Director Compensation.....	138
Making governance guidelines public	139
Evaluating the board's performance.....	139
Some Exempt Boards . . . For the Moment.....	140
Nonpublic companies	140
Nonprofit corporations.....	141
Other exempt companies	141

Chapter 10: SOX: Under New Management	143
Chiefly Responsible: CEOs and CFOs	143
CEO: The chief in charge	144
CFO: The financial fact finder	144
Three SOX sections for the chiefs	145
A Section 302 Certification Checklist	146
Paragraph 1: Review of periodic report	147
Paragraph 2: Material accuracy	147
Paragraph 3: Fair presentation of financial information	147
Paragraph 4: Disclosure controls and procedures	148
Paragraph 5: Disclosure to auditors	148
Paragraph 6: Changes in internal controls	149
Clearing Up Common Section 302 Questions	149
What companies are required to file certifications under Section 302?	150
Which reports get certified?	150
Viewing Control as a Criminal Matter: Section 906	151
More Reporting Responsibilities for Management and Auditors: Section 404	153
What management has to do under Section 404	153
What the auditors need from management	153
Taking Internal Control Seriously	154
Considering the auditor's perspective	154
What the SEC says	154
Management standards criteria for controls	155
Seeking Out Subcertifications	155
Some Good Advice for CEOs and CFOs	156
Establish a disclosure committee	157
Take an inventory	157
Woo the whistle-blowers	157
Chapter 11: More Management Mandates	159
Codifying the Corporate Conscience	159
Explaining the code	160
Establishing worthwhile objectives	160
Realizing one code doesn't fit all companies	160
Disclosing amendments and waivers	161
Expecting ethics on the exchanges	161
A checklist of code contents	161
New Rules for Stock Selling and Telling	162
Faster disclosure	163
More disclosure	163
Prohibiting Personal Loans	164
Banning Blackout Trading	164
Avoiding media images of stricken retirees	165
Making some necessary exceptions	165

Making Managers Pay Personally165
 The freeze factor.....166
 The danger of disgorgement166
 Stopping Audit Inference.....167
 Identifying audit interlopers167
 Suing audit interlopers168

Part III: Scaling Down Section 404 169

Chapter 12: Clearing Up Confusion about Control171

The Nuts and Bolts of Section 404171
 What Section 404 says172
 What Section 404 really does172
 SEC rules under Section 404173
 PCAOB participation in the Section 404 process173
 When Do Companies Have to Comply with Section 404?174
 Section 302 “Internal Control” versus Section 404 “Internal Control”175
 Defining “disclosure controls and procedures”
 under Section 302175
 Interpreting “internal control over financial reporting”
 under Section 404177
 Controlling the Cost of Compliance.....179
 Cost-cutting measures by the PCAOB179
 Section 404 sticker shock.....181
 Decreasing costs in year two181

Chapter 13: Surviving a Section 404 Audit183

Dividing Responsibilities in a Section 404 Audit183
 Management’s role184
 The independent auditor’s role184
 What Is (and Is Not) Related to the Audit185
 Complying with Auditing Standard No. 5186
 Integrating the audits.....186
 Planning the audits187
 Scaling the audits187
 Assessing the risk.....188
 Cutting costs by relying on the work of others188
 Using a top-down approach189
 Flunking a Section 404 Audit.....189
 How to fail a Section 404 audit189
 What to do if your company flunks.....190

Chapter 14: Taking the Terror Out of Testing 191

The Price of the Project.....191
 The six most common Section 404 project costs.....192
 Meeting massive manpower requirements192
 The social challenges of Section 404194

Hail to the Documenters	194
The right documentation skills	194
Getting the documentation down	195
Time tracking	195
Scoping out savings	196
Taking an inventory of your company processes	197
Organizing the documentation: Why form is equal to substance	200
Caveats about Controls	201
Key controls	202
Some common key controls	202
Ogling the Outside Vendors: SAS 70 Reports	203
Evaluating Control with the COSO Framework	204
How COSO breaks down companies' controls	204
COSO guidance for your company	205
A Bit about COBIT	205

***Part IV: SOX for Techies*.....207**

Chapter 15: Getting Technical with SOX209

Some Specific SOX Sections That Talk to Techies	210
Ramping up document retention policies	210
Disclosing critical events in real time.....	211
IT and the dreaded SOX Section 404.....	213
Getting a SOX-ified System in Place When . . .	213
. . . Your company is starting from scratch	214
. . . Your company is already halfway there	214
. . . Your company has a larger budget	214
Evaluating Your Systems after SOX	215
Organizing company data.....	215
Getting into the GAAP.....	216
Preventing Control Problems before They Happen.....	216
Spelling out security	216
Logging it all in.....	217
Falling Back on COBIT	217

Chapter 16: Surveying SOX Software219

Some SOX Software Trends.....	219
Identifying the Types of Software on the Market	221
Shopping for SOX Software	223
SOX Meets Cousin IT	224
Collecting scattered company data	225
Evaluating your company's existing IT systems	225
The COSO Standards for Software	228
Complying with COBIT	231

Chapter 17: Working with Some Actual SOX Software 233

Doing Your Research before a Software Installation	233
Tracking the flow of information in your company	234
Following the trial balance trail.....	236
Getting to Know SarbOxPro.....	236
The SarbOxPro checklist.....	238
The SarbOxPro data tree.....	239
SarbOxPro stages	239
Opting for Other Types of Software Solutions	245

Part V: To SOX-finity and Beyond..... 249**Chapter 18: Lawsuits under SOX 251**

The Smoking Gun: Knowledge.....	251
The First Big SOX Trial: Richard Scrushy	252
The squishy Scrushy facts	253
The prosecutors' post-game recap	254
The Scrushy epilogue: Civil suits, a tax refund, and a new trial...255	
Another Test of the "Ignorance" Defense: Kenneth Lay.....	255
Timing Is Everything: Andersen, Ernst, and KPMG	
Litigation Outcomes.....	257
Arthur Andersen's victory: Three years too late	258
An Ernst error	259
Kid gloves for KPMG?.....	260
The Gemstar Case: Interpreting Section 1103	261
Suing under SOX Section 304.....	261
Suing under Section 806: The Whistle-Blower Provision	262
Blowing the whistle before and after SOX.....	262
What happens when the whistle blows?.....	263
Tips for defending against whistle-blower suits.....	265

Chapter 19: The Surprising Scope of SOX 267

Outsourcing under SOX.....	267
Summarizing SAS 70	268
Sidestepping SAS 70	269
Extending SOX Principles to Not-for-Profits	269
SOX and Foreign Companies.....	271

Part VI: The Part of Tens..... 273**Chapter 20: Ten Ways to Avoid Getting Sued or
Criminally Prosecuted Under SOX 275**

Maintain an Active and Visible Audit Committee	275
Communicate about How to Communicate.....	276

Combat Policy Paranoia and Section 404 Audit-Chondria.....	276
Keep Bonuses within Bounds.....	277
Separate the Whistle-Blowers from the Whiners.....	277
Invest in IT Tools and Tricks.....	277
Do Something with All That Data.....	278
Disclose Triggering Events on Time.....	278
Document What's Delegated.....	278
Focus on Product and Service Delivery.....	279

Chapter 21: Ten Tips for an Effective Audit Committee 281

Pick the Right Number of Members.....	281
Set Up Subcommittees.....	282
Find a Financial Expert.....	283
Create Questionnaires.....	284
Adopt a Smart Charter.....	284
Keep Track of Complaints.....	285
Communicate Liberally.....	285
Report Annually.....	286
Identify Conflicts . . . and Nonconflicts.....	286
Give Notice When Needed.....	286

Chapter 22: Ten Smart Management Moves 289

Form a Disclosure Committee.....	289
Set Reporting Schedules.....	290
Have More Meetings and Send Less E-mail.....	290
Challenge Outdated and Overly Detailed Policies.....	291
Review Reports with Their Preparers.....	291
Keep Up with Current Certification Requirements.....	292
Avoid Animosity with the Audit Committee.....	292
Don't Confuse Certification with Control.....	293
Consider Getting Subcertifications.....	293
Track All the Timelines.....	293

Chapter 23: Ten Things You Can't Ask an Auditor to Do After SOX . 295

Keep Your Books.....	296
Fix Your Financial Information Systems.....	296
Appraise Company Property.....	297
Act as an Actuary.....	297
Perform Internal Audit Services for Your Company.....	297
Fill In for Your Management Team.....	298
Be a Headhunter.....	298
Advise You on Investments.....	299
Dispense Legal Advice.....	299
Give You an Expert Opinion.....	299

Chapter 24: Top Ten Places to Get Smart about SOX 301

Sample SOX-online.....	301
Peruse the PCAOB Web Site.....	302

Visit the SEC Web Site.....302
 Get Inside Sarbanes-Oxley Trenches302
 Link to the AICPA Web Site.....304
 Frequent the Forum304
 Click On the COSO Web Site304
 Find the FEI Web Site304
 Spring for a Subscription to Compliance Week.....305
 Don't Forget Wikipedia!305

Part VII: Appendixes.....307

Appendix A: Selected Sections, Auditing Standard No. 5 309

Introduction309
 Integrating the Audits.....310
 Role of Risk Assessment.....310
 Scaling the Audit311
 Addressing the Risk of Fraud.....311
 Using the Work of Others311
 Using a Top-Down Approach312

Appendix B: Sample Certifications 313

Sample General Section 302 Certification313
 Sample Section 906 Certification.....315
 Sample Subcertification of Employee.....315

Appendix C: Sample Audit Committee Charter 319

Audit Committee Charter.....319
 Purpose.....319
 Authority320
 Composition.....322
 Meetings322
 Responsibilities322

Appendix D: Sample Code of Ethics 329

Business Conduct and Ethics Policy329
 Policy329
 Scope.....329
 Responsibility329
 Provisions.....330

Appendix E: Sample SAS 70 Report 337

Index.....339

Introduction

Welcome to *Sarbanes-Oxley For Dummies*, 2nd Edition. Whether you're a CEO or CFO, governance officer, CPA, manager, entrepreneur, file clerk, or cleric, this book is for you. It's designed to tell you where you fit into the grand scheme of corporate compliance and why you're being asked to do what you do by your board of directors, banker, customers, and clients.

Having the big picture straight in your mind helps ensure that you won't lose track of the minutiae and details that accompany the sweeping piece of legislation that is Sarbanes-Oxley, whether you're gearing up for initial compliance or attempting to streamline in subsequent years. If you're part of a private company or not-for-profit, I offer special congratulations to you. After all, you're savvy enough to know that Sarbanes-Oxley is here to stay and that it's becoming the gold standard for fair, ethical, and efficient business practices (whether you're obligated to comply or not).

About This Book

The Sarbanes-Oxley Act, or SOX as it's affectionately called in the world of corporate governance, is a responsive piece of legislation. Like the securities laws passed in the 1930s, SOX was passed in response to a real crisis and to genuine public outrage. It sailed through Congress on a wave of bipartisan support surprisingly free of lobbying and loophole legislating. Instead, Congress left the details to the Securities and Exchange Commission (SEC) and the newly created Public Company Accounting Oversight Board (PCAOB). This book walks you through SOX's rather piecemeal rules and pronouncements and gives you a sense of how to anticipate future trends and traps in this area of the law.

The goal of *Sarbanes-Oxley For Dummies*, 2nd Edition, is to give you a helicopter view of the regulatory terrain while helping you focus a beam on the key details of the legislation. This book is intended to give you a sophisticated understanding of the purpose and structure of the legislation as it affects many disciplines and areas of the law. This book is sure to empower you with the level of insight you need for practical, cost-effective decision-making. It will assist you with the following:

- ✓ **Understanding why SOX was passed:** Looking at the kind of conduct SOX was intended to combat can help you create meaningful standards for the company with which you work or are affiliated.

- ✔ **Instituting cost-effective compliance with SOX:** This book's practical view of the legislation can keep you from becoming bogged down in regulatory details and allowing lawyers and accountants to go off on expensive tangents that have little to do with the essence of SOX.
- ✔ **Finding answers on specific SOX issues:** This book explains how and where to find SEC rules and pronouncements that are critical to implementation of SOX and translates those rules into plain English.
- ✔ **Avoiding lawsuits and regulatory actions:** This book, although not intended to be a substitute for a good securities lawyer or a CPA, takes a hard look at who gets sued under SOX and how you can avoid having your company or yourself added to the list of litigants.
- ✔ **Anticipating future rules and trends:** SEC rules and PCAOB pronouncements under SOX continue to be issued with regularity. But with a comprehensive understanding of what the law is designed to do, you'll be less surprised by what's ultimately issued.

Conventions Used in This Book

It's unfortunate, but understanding SOX means that you're going to run into lots of legal jargon and accounting minutiae. To give you a jump start, I define some legal and accounting terms in this book and use *italic* font to make such terms stand out a bit. I also use **boldfaced** words to highlight key words in bulleted lists and numbered steps. `Monofont` indicates Web addresses, which I refer to often.

When this book was printed, some Web addresses may have needed to break across two lines of text. If that happened, rest assured that we haven't put in any extra characters (such as hyphens) to indicate the break. So, when using one of these Web addresses, just type in exactly what you see in this book, pretending as if the line break doesn't exist.

What You're Not to Read

I occasionally wander off-topic to discuss something historical, technical, or interesting (or, at least, interesting to me!). In these instances, I set the discussions apart by placing them in sidebars, which are the gray boxes you'll see from time to time throughout the book. Because the text in sidebars is nonessential, feel free to skip it if it doesn't interest you.

Foolish Assumptions

When writing this book, I had to make a few assumptions about who my readers would be and what kind of information they'd be looking for. This section explains those assumptions. For example, I assume you want to understand the Sarbanes-Oxley Act in a way you can't achieve by suffering through the 80-some pages of the statute and 1,000 or so pages of related congressional hearings. You want to make sure you have a handle on the important aspects of the legislation, how it affects you and your company, and how companies can comply most cost-effectively.

Additionally, if you're a service provider such as a lawyer or CPA, I assume that you're looking for insight into the following tasks — insights you would glean from the legal and accounting professionals involved in writing this book (whose credentials and accomplishments are listed on the acknowledgments page):

- ✓ Recognizing and creating a legally effective, fully compliant corporate governance framework
- ✓ Determining what aspects of SOX apply to your company or should be voluntarily adopted by your company (whether it's publicly traded, privately held, or not-for-profit)
- ✓ Managing and streamlining Section 404 compliance as well as seizing opportunities and benefiting from information resulting from the unprecedented testing and documentation of business processes all across the United States
- ✓ Interpreting media accounts, court cases, and economic projections involving SOX

How This Book Is Organized

Sarbanes-Oxley is an extremely broad piece of legislation, spanning legal, accounting, and information technology disciplines, so this book is chock-full of information. But not to worry: The index and table of contents will help you find your way. The chapters in this book treat each topic independently without assuming you've read previous chapters (as a textbook might), so you can use them as references and jump around to find what you need. This book is divided into six parts, which I explain in the following sections.

Part I: The Scene Before and After SOX

This part of the book starts at the beginning, explaining why SOX was passed and taking you on a tabloid tour of the corporate scandals that inspired it — Enron, WorldCom, Adelphia, Global Crossing, and more. These chapters shock you with tales of greed and manipulation and walk you section-by-section through the legislation, explaining what each provision is intended to accomplish.

Part II: SOX in the City: Meeting New Standards

The chapters in this part spell out who's affected by which provisions. You find out why the accounting profession is no longer self-regulating, and you're introduced to the new audit ambience that SOX provides. You also get a good look at what SOX means for management, including what's expected of boards and the committees formed under their direction.

Part III: Scaling Down Section 404

SOX Section 404 is a big enough deal to warrant its own part in this book. These chapters take you by the hand and guide you through the dreaded Section 404 audit process. They tell you how to manage a Section 404 project and when and how to cut compliance costs without cutting corners.

Part IV: SOX for Techies

This part is all about software. It explains how software can help you comply with SOX and what to look for when investing in information technology to carry out SOX objectives. These chapters show you some of the more cost-effective products on the market and suggest particularly useful systems for small to mid-size companies.

Part V: To SOX-finity and Beyond

This part looks at the future of SOX and corporate governance. These chapters take you into the courtroom to see who's getting sued under SOX and what the outcomes are. This part also looks at what SOX means for outsourced services and service providers and explains when special SAS 70 reports are required (as well as when they aren't).