

Now updated! Your guide to the latest
SOX legislation and compliance requirements

Sarbanes-Oxley

FOR DUMMIES[®]

2nd Edition

Strategies for
staying public
or going private

**A Reference
for the
Rest of Us![®]**

FREE eTips at dummies.com[®]

**Jill Gilbert Welytok,
JD, CPA**
Attorney and Sarbanes-Oxley Consultant



**Now updated! Your guide to the latest
SOX legislation and compliance requirements**

Sarbanes-Oxley

FOR **DUMMIES**[®]

2nd Edition

**Strategies for
staying public
or going private**

**A Reference
for the
Rest of Us!**[®]

FREE eTips at dummies.com

**Jill Gilbert Welytok,
JD, CPA**
Attorney and Sarbanes-Oxley Consultant



***Sarbanes-Oxley For
Dummies, Second Edition***

**by Jill Gilbert Welytok,
JD, CPA**



WILEY

Wiley Publishing, Inc.

Sarbanes-Oxley For Dummies, Second 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 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>.

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 877-762-2974, 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



About the Author

Jill Gilbert Welytok, JD, CPA, LLM, practices in the areas of corporate, nonprofit 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, LLM – 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

Title

[Introduction](#)

[About This Book](#)

[Conventions Used in This Book](#)

[What You're Not to Read](#)

[Foolish Assumptions](#)

[How This Book Is Organized](#)

[Icons Used in This Book](#)

[Where to Go from Here](#)

[Feedback, Please](#)

[Part I : The Scene Before and After SOX](#)

[Chapter 1: The SOX Saga](#)

[Plowing Through the Politics of SOX](#)

[Combating Corruption under SOX: Everyone Has a Role](#)

[A Summary of SOX: Taking It One Title at a Time](#)

[Some Things SOX Doesn't Say: SOX Myths](#)

[Chapter 2: SOX in Sixty Seconds](#)

[Reestablishing Control after the Scandals](#)

[Four Squeaky Clean SOX Objectives](#)

[How SOX Protects the Investing Public](#)

[Rapid Rulemaking Regrets](#)

[Chapter 3: SOX and Securities Regulations](#)

[Pre-SOX Securities Laws](#)

[The Scope of SOX: Securities and Issuers](#)

[The Post-SOX Paper Trail](#)

[Behind the 8-K Ball after SOX](#)

[Annual SEC Scrutiny after SOX](#)

[Why Privately Held Companies Care about SOX](#)

[Chapter 4: SOX and Factual Financial Statements](#)

[Auditing the Auditors: 2007 Guidance from the SEC](#)

[SOX's Recipe for Seeking Out Cooked Books](#)

[Finding Financial Information](#)

[Accessing Annual Reports](#)

[Surfing SEC Filings](#)

[Chapter 5: What's New for Non- Accelerated Filers](#)

[A SOX Update for Small Companies](#)

[Getting the Auditor's Opinion](#)

[Part II : SOX in the City: Meeting New Standards](#)

[Chapter 6: A New Audit Ambience](#)

[How SOX Rocks the Accounting Profession](#)

[An Example of Audit Failure: Arthur Andersen](#)

[SOX as a Substitute for Self-Regulation](#)

[Is There an Independent Auditor in the House?](#)

[What SOX Says to CPAs](#)

[Section 404: The Sin Eater Provision](#)

[Chapter 7: A Board to Audit the Auditors](#)

[Taking a New Approach to Audit Oversight](#)

[Primary Purposes of the PCAOB](#)

[Some Practical PCAOB Matters](#)

[PCAOB Rules: Old Meets New](#)

[Evolving PCAOB Policies and Issues](#)

[When the PCAOB Doesn't Perform](#)

[Struggling for Standards](#)

[Chapter 8: The Almighty Audit Committee](#)

[Deliver or Delist: Rules of the Stock Exchanges](#)

[From the Audit Committee Annals](#)

[Starting with a Charter](#)

[The Audit Committee Interface](#)

[Some Stricter NYSE Rules](#)

[Membership Requirements](#)

[Day-to-Day Committee Responsibilities](#)

[Chapter 9: Building Boards That Can't Be Bought](#)

[Some Background about Boards](#)

[In Search of Independent Directors](#)

[Forming Committees for Nominating Directors](#)

[Regulating Director Compensation](#)

[Some Exempt Boards . . . For the Moment](#)

[Chapter 10: SOX: Under New Management](#)

[Chiefly Responsible: CEOs and CFOs](#)

[A Section 302 Certification Checklist](#)

[Clearing Up Common Section 302 Questions](#)

[Viewing Control as a Criminal Matter: Section 906](#)

[More Reporting Responsibilities for Management and Auditors: Section 404](#)

[Taking Internal Control Seriously](#)

[Seeking Out Subcertifications](#)

[Some Good Advice for CEOs and CFOs](#)

[Chapter 11: More Management Mandates](#)

[Codifying the Corporate Conscience](#)

[New Rules for Stock Selling and Telling](#)

[Prohibiting Personal Loans](#)

[Banning Blackout Trading](#)

[Making Managers Pay Personally](#)

[Stopping Audit Inference](#)

[Part III : Scaling Down Section 404](#)

[Chapter 12: Clearing Up Confusion about Control](#)

[The Nuts and Bolts of Section 404](#)

[When Do Companies Have to Comply with Section 404?](#)

[Section 302 “Internal Control” versus Section 404 “Internal Control”](#)

[Controlling the Cost of Compliance](#)

[Chapter 13: Surviving a Section 404 Audit](#)

[Dividing Responsibilities in a Section 404 Audit](#)

[What Is \(and Is Not\) Related to the Audit](#)

[Complying with Auditing Standard No. 5](#)

[Flunking a Section 404 Audit](#)

[Chapter 14: Taking the Terror Out of Testing](#)

[The Price of the Project](#)

[Hail to the Documenters](#)

[Caveats about Controls](#)

[Ogling the Outside Vendors: SAS 70 Reports](#)

[Evaluating Control with the COSO Framework](#)

[A Bit about COBIT](#)

[Part IV : SOX for Techies](#)

[Chapter 15: Getting Technical with SOX](#)

[Some Specific SOX Sections That Talk to Techies](#)

[Getting a SOX-ified System in Place When . . .](#)

[Evaluating Your Systems after SOX](#)

[Preventing Control Problems before They Happen](#)

[Falling Back on COBIT](#)

[Chapter 16: Surveying SOX Software](#)

[Some SOX Software Trends](#)

[Identifying the Types of Software on the Market](#)

[Shopping for SOX Software](#)

[SOX Meets Cousin IT](#)

[The COSO Standards for Software](#)

[Complying with COBIT](#)

[Chapter 17: Working with Some Actual SOX Software](#)

[Doing Your Research before a Software Installation](#)

[Getting to Know SarbOxPro](#)

[Opting for Other Types of Software Solutions](#)

[Part V : To SOX-finity and Beyond](#)

[Chapter 18: Lawsuits under SOX](#)

[The Smoking Gun: Knowledge](#)

[The First Big SOX Trial: Richard Scrushy](#)

[Another Test of the “Ignorance” Defense: Kenneth Lay](#)

[Timing Is Everything: Andersen, Ernst, and KPMG Litigation Outcomes](#)

[The Gemstar Case: Interpreting Section 1103](#)

[Suing under SOX Section 304](#)

[Suing under Section 806: The Whistle-Blower Provision](#)

[Chapter 19: The Surprising Scope of SOX](#)

[Outsourcing under SOX](#)

[Extending SOX Principles to Not-for-Profits](#)

[SOX and Foreign Companies](#)

[Part VI : The Part of Tens](#)

[Chapter 20: Ten Ways to Avoid Getting Sued or Criminally Prosecuted Under SOX](#)

[Maintain an Active and Visible Audit Committee](#)

[Communicate about How to Communicate](#)

[Combat Policy Paranoia and Section 404 Audit-Chondria](#)

[Keep Bonuses within Bounds](#)

[Separate the Whistle-Blowers from the Whiners](#)

[Invest in IT Tools and Tricks](#)

[Do Something with All That Data](#)

[Disclose Triggering Events on Time](#)

[Document What’s Delegated](#)

[Focus on Product and Service Delivery](#)

[Chapter 21: Ten Tips for an Effective Audit Committee](#)

[Pick the Right Number of Members](#)

[Set Up Subcommittees](#)

[Find a Financial Expert](#)

[Create Questionnaires](#)

[Adopt a Smart Charter](#)

[Keep Track of Complaints](#)

[Communicate Liberally](#)

[Report Annually](#)

[Identify Conflicts . . . and Nonconflicts](#)

[Give Notice When Needed](#)

[Chapter 22: Ten Smart Management Moves](#)

[Form a Disclosure Committee](#)

[Set Reporting Schedules](#)

[Have More Meetings and Send Less E-mail](#)

[Challenge Outdated and Overly Detailed Policies](#)

[Review Reports with Their Preparers](#)

[Keep Up with Current Certification Requirements](#)

[Avoid Animosity with the Audit Committee](#)

[Don't Confuse Certification with Control](#)

[Consider Getting Subcertifications](#)

[Track All the Timelines](#)

[Chapter 23: Ten Things You Can't Ask an Auditor to Do After SOX](#)

[Keep Your Books](#)

[Fix Your Financial Information Systems](#)

[Appraise Company Property](#)

[Act as an Actuary](#)

[Perform Internal Audit Services for Your Company](#)

[Fill In for Your Management Team](#)

[Be a Headhunter](#)

[Advise You on Investments](#)

[Dispense Legal Advice](#)

[Give You an Expert Opinion](#)

[Chapter 24: Top Ten Places to Get Smart about SOX](#)

[Sample SOX-online](#)

[Peruse the PCAOB Web Site](#)

[Visit the SEC Web Site](#)

[Get Inside Sarbanes-Oxley Trenches](#)

[Link to the AICPA Web Site](#)

[Frequent the Forum](#)

[Click On the COSO Web Site](#)

[Find the FEI Web Site](#)

[Spring for a Subscription to Compliance Week](#)

[Don't Forget Wikipedia!](#)

[Part VII : Appendixes](#)

[Appendix A: Selected Sections, Auditing Standard No. 5](#)

[Appendix B: Sample Certifications](#)

[Sample General Section 302 Certification](#)

[Sample Section 906 Certification](#)

[Sample Subcertification of Employee](#)

[Appendix C: Sample Audit Committee Charter](#)

[Audit Committee Charter](#)

[Appendix D: Sample Code of Ethics](#)

[Business Conduct and Ethics Policy](#)

[Appendix E: Sample SAS 70 Report](#)

: Further Reading

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.