Manager's Guide to Compliance

Sarbanes-Oxley, COSO, ERM, COBIT, IFRS, BASEL II, OMB A-123, ASX 10, OECD Principles, Turnbull Guidance, Best Practices, and Case Studies

ANTHONY TARANTINO

WILEY

John Wiley & Sons, Inc.

This book is printed on acid-free paper. ♾

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

Published simultaneously in Canada.

For general information on our other products and services, or 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 http://www.wiley.com.

Library of Congress Cataloging-in-Publication Data

Tarantino, Anthony, 1949-

Manager's guide to compliance : Sarbanes-Oxley, COSO, ERM, COBIT, IFRS, BASEL II, OMB A-123, ASX 10, OECD principles, Turnbull guidance, best practices, and case studies / Anthony Tarantino.

p. cm.

Includes index.

ISBN-13: 978-0-471-79257-4 (cloth)

ISBN-10: 0-471-79257-8 (cloth)

1. Accounting—Law and legislation—United States. 2. Auditing, Internal—Law and legislation—United States. 3. Disclosure of information—Law and legislation—United States. 4. Accounting—Standards. 5. Auditing, Internal—Standards. I. Title.

KF1357.T37 2006

346.73'06648--dc22

2005034272

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

Dedicated
to
Ted and Allie

NOTE TO THE READER

Contents

Preface

The massive U.S. corporate scandals of the last several years have led to a huge change in the way organizations are governed. At its heart was a failure of leadership, ethics, and morality on several levels, which led to a breakdown in investor confidence. The failures occurred among corporate executives, boards of directors, regulatory agencies, rating agencies, and the press. One could argue this was caused by a lack of virtue and a breaking of a social contract between organizations (public and private) and those who invest in and rely on them. These are age-old concepts. In his *Analects*, the great Chinese sage Confucius (551–479 B.C.) argued virtue was the key characteristic of superior leadership. Virtue provides a moral power that allows one to win a following without resorting to physical force and enables a leader to maintain good order. Mencius (372–289 B.C.), is often referred to as the second great Chinese sage, and he developed the notion of a social contract in which one rules by a mandate of heaven. If a leader broke the social contract, then his followers would be absolved of all loyalty and might be required to overthrow him. Enron, WorldCom, Parmalat, Ahold, and others broke the mandate of heaven in corporate America and Europe and exposed the lack of virtue in those entrusted with good corporate governance.

These events have spawned a move toward more robust compliance on a global level, which will require much improved internal controls and will change the nature of business in fundamental ways. The struggle for improved compliance is nothing new. Investors have always sought greater transparency as organizations have sought to limit transparency to protect competitive information. Scandals have always acted as a catalyst to force improved corporate governance and transparency. The South Sea Bubble scandal in the early 1700s fostered improved accounting standards in British companies. U.S. states began enacting blue-sky laws in the early 1900s as the result of shady stock promotions. Of course, the greatest reforms came as a result of the great stock market crash of 1929 and depression during the 1930s. This led to the passage of federal security legislation in 1933 and 1934 and the creation of the Securities and Exchange Commission (SEC).[1] Reforms have continued, but were greatly accelerated by scandals of the late 1990s. So there is little chance for a significant rollback in compliance requirements, especially when most investors do not place much faith in corporate boards to provide viable oversight. A Wall Street Journal/Harris poll found about two-thirds of investors expressing doubts in the ability of corporate boards of directors to provide effective oversight.[2]

Many skeptics have made analogies with Year 2000 (Y2K) and International Organization for Standardization (ISO) certifications, suggesting that this is only a passing fad or an American-based overreaction to Enron-type scandals. Though the argument about an overreaction has some merit, this is no passing fad. Though the U.S. Sarbanes-Oxley Act (SOX) has received the lion's share of attention, initiatives are underway in almost every global region and industry to improve transparency in financial reporting. In spite of ongoing complaints from U.S. companies above excessive compliance costs, the Wall Street Journal/Harris online poll found that most U.S. investors still believe corporate governance regulations remain too lenient. The same poll found only 6% of investors believing corporate governance to be too strict. This skepticism about the effectiveness of corporate governance has led nearly one-third of investors to reduce or to divest their stake in various companies due to concerns about the quality of their corporate governance.[3]

The reasons for the wave of compliance initiatives and the need for improved internal controls are simple. We are fast approaching a global marketplace in which investors will demand a level playing field in comparing financial results whether companies or industries are based in the United States, the European Union (EU), Russia, China, or other Third World countries. Privates and nonprofits are feeling the pressure to improve internal controls from their insurers and bankers if they want to get the most competitive rates. This is not

[1]John Emshwiller, "Opening the Books," *Wall Street Journal,* October 17, 2005.
[2]Becky Bright, "Investors Are Skeptical of Success of Sarbanes-Oxley, Poll Finds," Wall Street Journal/Harris On Line Poll, October, 14, 2005.
[3]Becky Bright, "Investors Are Skeptical of Success of Sarbanes-Oxley, Poll Finds," Wall Street Journal/Harris On Line Poll, October, 14, 2005.

to say bumps will not occur along the way. Years of sloppy business practices, weak internal and external audits, and lackluster enforcement will make this a painful process. In Third World countries where most businesses are family run and/or closely held, this will present additional challenges.

A major debate is underway as to whether mandatory government regulations with severe criminal and criminal penalties, such as SOX, are needed to improve governance and internal controls, or whether principles-based guidelines, advocated in Europe, will suffice. New York's Attorney General, Eliot Spitzer, has referenced President Teddy Roosevelt, who advocated 100 years ago that government alone must oversee marketplaces and that self-regulation was doomed to fail. "Teddy Roosevelt understood the marketplace . . . that in order to preserve dynamism in the marketplace there needed to be that force to ensure competition and a level playing field," he says. "That's the role we play on Wall Street. That's what we've done in terms of labor markets and the environment."[4]

The major U.S. scandals at Enron, Tyco, WorldCom, Riggs Banks, Fannie Mae, ImClone, HealthSouth, Marsh & McClennan, and European scandals at Ahold and Parmalat would suggest the futility of voluntary measures, but it is still early in the process and not yet clear if SOX will have the desired effect and the benefits will outweigh the costs. Post-SOX scandals such as Refco, the largest independent futures brokerage firm, will also raise the debate that all the detailed oversight and higher audit standards can still miss major corruption, in this case poor due diligence for Refco's August 2005 IPO.[5]

Today's managers face a growing challenge and dilemma in the global thrust to improve governance and compliance, which at its core requires robust internal controls. The dilemma comes in how to comply in a manner that does not punish operational efficiencies and competitiveness. This will be true for privately and publicly held companies throughout the globe and even for nonprofit institutions. Down to the U.S. state level (California's AB 1386 protects individual identities) and at federal government agency level (US OMB's A-128 applies SOX to federal agencies), compliance initiatives will become

[4]Michael Gormley, "Gangbuster to Governor? New York's Attorney General Starts Down a Familiar Path," Associated Press, Sunday, June 13, 2004.
[5]Julie Johnsson, "Chicago's Grant Thornton Sued Over Refco Scandal," *Chicago Business,* Oct. 13, 2005.

role models bound to spread to other U.S. states, local government agencies, and international governments.

The good news in global compliance efforts is the acceptance of COSO-like standards to improve internal controls. Improved internal controls are at the core of almost all compliance regulations. Though a healthy debate continues between the use of voluntary guidelines versus compulsory regulations, there is widespread acceptance for the need to improve internal controls using the Committee of Sponsoring Organizations (COSO) definition and approach. COSO used a commonsense approach to internal controls, which includes defining and categorizing the criticality of business processes, the risks associated with business processes, and the means to mitigate risks. The mitigation process includes assigning its owners, and then testing, auditing, and certifying the adequacy of controls.

We will begin with an introduction to SOX, which is technically called the Public Company Accounting Reform and Investor Protection Act of 2002. SOX was sponsored by Senator Paul Sarbanes (Democrat–Maryland), then chairman of the Committee on Banking, Housing and Urban Affairs in the Senate, and Representative Michael Oxley (Republican–Ohio), the Financial Services Committee chair in the House. It passed the Senate unanimously, won easy approval in the House, and President Bush signed it into law on July 30, 2002. The internal control provisions went into effect for larger companies in 2004. Smaller companies and foreign filers are given more time, with deadlines pushed from July 2005 to July 2007.

The SEC has delivered several final rulings defining its SOX interpretation. Based on the final rulings, the intent is to expand rather than to limit the reach of the act. William H. Donaldson, the former chairman of the SEC, made it clear in his September 2003 testimony, that SOX is essential in restoring investor confidence by providing transparency in financial reporting. He summarized the events of the 1990s and made an ominous comparison with the events of 1929: "The low points in this story are now household names, not just Enron, but also WorldCom, Tyco, Adelphia, and others. There was other serious misconduct as well, including in the once-celebrated IPO market, which in too many cases lacked both fairness and integrity. The cost of this corner cutting to investors has been enormous. While thankfully we have not witnessed the same intensity of human suffering that came with the depression of the 1930s, the most recent downturn in the market directly affected many more investors than the

1929 market crash, because many more individuals had much more of their savings invested in the stock market."[6]

We will provide a more detailed look at SOX Sections 401, 404, 406, and 409 and then discuss the impact of SOX on small and foreign filers, privates, and nonprofits. This will be followed by an overview of SOX-like legislation coming to U.S. federal agencies, Australia, Canada, and the UK. We will include a discussion of efforts to improve internal controls in the following industries: health (HIPPA), banking (GLB and Basel II), and insurers (Solvency II). The movement to create principles-based guidelines by the OECD and global Generally Accepted Accounting Principles (GAAP) by the IFRS will be compared to SOX and U.S. GAAP. The impact on outsourcing will include an explanation of the Statement on Auditing Standards No. 70 (SAS 70) audit process. The civil and criminal penalties for noncompliance will demonstrate the major changes brought about by the U.S. corporate scandals. Best practices in internal controls will be offered that include several case studies and the role technology can play in automating compliance. Finally, we will provide a cost versus benefits analysis. This text is designed to be an introductory guide and handbook for professionals in information technology (IT), operations, finance, and supply chain. It may be helpful to internal and external auditors but is not designed to provide a framework for the audit process. It may help regulators as a high-level overview of the many compliance and governance initiatives underway throughout the world. Finally, it may also be helpful to investors who seek to evaluate the merits of the compliance initiatives in mitigating risks in companies, industries, and regions they are considering.

Note: Throughout the text we have used auditing examples and case studies around the procure-to-pay (P2P) process since it is typically well understood by accounting, operations, and IT professionals.

Anthony Tarantino
April 2006

---

[6]Testimony Concerning Implementation of the Sarbanes-Oxley Act of 2002, by William H. Donaldson, Chairman U.S. Securities and Exchange Commission. Before the Senate Committee on Banking, Housing and Urban Affairs, September 9, 2003, http://www.sec.gov/news/testimony/090903tswhd.htm.

ACKNOWLEDGMENTS

The author gratefully acknowledges the following individuals for their invaluable input and expertise:

Koti Ancha, MSIE, Six Sigma Black Belt, Senior Program Manager, Supply Chain Strategy, Seagate Technology, Scotts Valley, CA. For assistance in providing case studies and general editing.

Mark Stebelton, CPA, Senior Program Manager, Compliance Softwares and SOX SME, Logical Apps, Irvine, CA. For sharing expertise, specifically regarding SAS 70.

Holly Tran, CISSP, CISM, MSEE, Manager, BearingPoint. For system security and compliance practice support.

Greg Henzel, MBA, Manager, BearingPoint. For contributions to mapping the following standards: COSO, ERM, and PCAOB.

Richard Marti, Manager, BearingPoint. For contributions to mapping the following standards: COSO, ERM, and PCAOB.

Shirley Cui, MSCS. For indexing and general editing support.

CHAPTER 1

U.S. SOX Section 401: Off-Balance Sheet Arrangements

INTRODUCTION[1]

Christopher Cox replaced William Donaldson as SEC Chairman in 2005. Since assuming his chairmanship, Cox has advocated a rethinking of regulations, arguing that they are overly complex and this complexity is partly to blame for the accounting scandals of the 1990s. Maybe the best evidence of this is the convoluted and confusing regulations and guidance around off-balance sheet (OBS) arrangements. This chapter will detail the current state of the U.S. regulations. It appears that the current regulations invite abuse and misunderstanding, and do not assure investors that Enron-type abuses are a thing of the past.

Section 401 of the Sarbanes-Oxley Act of 2002 requires the listing of off-balance sheet (OBS) arrangements, transactions, and obligations (including contingent obligations) that may have a material effect, current or future, on financial conditions, changes in financial results in operations, liquidity capital expenditures, capital resources, or significant components or revenues or expenses. The SEC final ruling requires the disclosure of "the nature and business purpose of the OBS arrangements, why and how they are needed in running a business." For those wondering why this is an area of concern, a one-word explanation should suffice—Enron. It was Enron's horrible abuse, and Arthur Andersen's blessing such OBS arrangements, that led to the most infamous and globally recognized scandal in a generation.

The problems stem from the complexity and resulting confusion in how to account for OBS arrangements. Unfortunately, the SEC has not simplified the process to the extent to preclude significant abuse.

Even a process as seemingly straightforward as procurement is given alternative interpretations. With U.S. GAAP's taking a rules-based approach (as opposed to principles-based as favored by the International Financial Reporting Standards (IFRS)), it is curious how rules and guidance can be issued which are not clear and straightforward. One cynical interpretation is that the complexity is by design serving those who make their living interpreting the regulations and those using the complexity of the regulations to minimize their tax exposure. A less cynical interpretation is that U.S. tax law continues to evolve to the point that even the brightest financial experts struggle in understanding it.

After reading this section, ask yourself if these regulations are straightforward enough to assure their consistent application by companies of all sizes and complexities and to avoid Enron-type abuses of the past.

The following are some simple examples of OBS obligations that may need to be accounted for:

- **Long-Term Purchase Agreements**: Common practice is to use long-term purchase agreements to assure a reliable source of supply for goods and services at the lowest price. Many companies are moving their direct material programs to Vendor/Supplier Managed Inventory (VMI) programs, which are controlled by long-term purchase agreements. Section 401 clearly requires a time-phased listing of obligations (Year 1, Years 2–3, etc.) in a tabular format specified by the SEC.
- **Cancellation and Restocking Charges**: Though the SEC is clear in defining the requirement to list time-phased obligations, restocking and cancellation charges are not mentioned specifically in Section 401 but are listed as new triggering events requiring an 8-K filing "any material early termination penalties" under Section 409. Most long-term agreements include such provisions. Though the SEC's intent is unclear, a company suffering a major downturn and paying restocking and/or cancellation charges will have trouble defending not listing these as OBS obligations.
- **Lease Agreements**: In addition to the aforementioned items, Capital and Operating Lease obligations should be listed as OBS obligations. Fees incurred due to early termination of agreements will need to be accounted for as well.

Even more complex is the requirement to account for contingent OBS obligations. The SEC provides an instruction "that a company must provide the disclosure required regarding off-balance sheet arrangements, whether or not the company is also a party to the transaction or agreement creating the contingent obligation arising under the off-balance sheet arrangement. In the event that neither the company nor any affiliate of the company is a party to the transaction or agreement creating the contingent obligation arising under the off-balance arrangement in question, the four-business-day period for reporting the event under this item would begin on the earlier of

- The fourth business day after the contingent obligation is created or arises, and
- The day on which an executive officer of the company becomes aware of the contingent obligation."

This has major ramifications for those enterprises that sell through channel partners with indirect channel sales agreements. OBS obligations may exist for consignment inventory, returns, rebate programs with volume incentives, warranty, special pricing agreements, and so on. Contingent OBS obligations may come into play for those who have outsourced manufacturing, distribution/logistics, and design.

Obviously stung by the terrible abuses of Enron, the SEC has laid out a comprehensive process for companies to explain OBS transactions and obligations.

The SEC's definition of OBS arrangements addresses certain guarantees that may be a source of potential risk to a company's future liquidity, capital resources, and results of operations, regardless of whether or not they are recorded as liabilities. The SEC has ruled that this may include "contracts that contingently require the guarantor to make payments to the guaranteed party based on another entity's failure to perform under an obligating agreement (e.g., a performance guarantee)."

Accounting for OBS arrangements is not enough. The SEC has ruled that companies will have to explain the nature and business purpose of such arrangements. "The disclosure should explain to investors why a company engages in off-balance sheet arrangements and should provide the information that investors need to understand the business activities advanced through a company's off-balance sheet arrangements. For example, a company may indicate that the arrangements enable the company to lease certain facilities rather than acquire them, where the latter would require the company to recognize a liability for the financing. Other possible disclosures under this requirement may indicate the off-balance sheet arrangement enables the company to obtain cash through sales of groups of loans to a trust; to finance inventory, transportation, or research and development costs without recognizing a liability; or to lower borrowing costs of unconsolidated affiliates by extending guarantees to their creditors."

The SEC requires companies to explain the impact on their "liquidity, capital resources, market risk support, credit risk support or other benefits. This disclosure should provide investors with an understanding of the importance of off-balance sheet arrangements to the company as a financial matter . . . . Together with the other disclosure requirements, companies should provide information sufficient for investors to assess the extent of the risks that have been transferred and retained as a result of the arrangements."

The SEC goes further. "In addition, the disclosure should provide investors with insight into the overall magnitude of a company's off-balance sheet activities, the specific material impact of the arrangements on a company, and the circumstances that could cause material contingent obligations or liabilities to come to fruition. Disclosure is required to the extent material and necessary to investors' understanding of

- The amounts of revenues, expenses, and cash flows of the company arising from the arrangements,
- The nature and total amount of any interests retained, securities issued and other indebtedness incurred by the company in connection with such arrangements, and
- The nature and amount of any other obligations or liabilities (including contingent obligations or liabilities) of the company arising from the arrangements that is, or is reasonably likely to become, material and the triggering events or circumstances that could cause them to arise."

DEFINITION OF OBS ARRANGEMENTS[2]

The SEC has defined the term OBS arrangement as "any transaction, agreement or other contractual arrangement to which an entity that is not consolidated with the company is a party, under which the company, whether or not a party to the arrangement, has, or in the future may have:

- Any obligation under a direct or indirect guarantee or similar arrangement,
- A retained or contingent interest in assets transferred to an unconsolidated entity or similar arrangement,
- Derivatives, to the extent that the fair value thereof is not fully reflected as a liability or asset in the financial statements, and
- Any obligation or liability, including a contingent obligation or liability, to the extent that it is not fully reflected in the financial statements (excluding the footnotes thereto)."

In particular, the proposals require a disclosure where the likelihood of the occurrence of a future event implicating an OBS arrangement or its material effect was higher than remote. As mentioned above, the SEC noted, "the disclosure threshold departed from the existing MD&A threshold, under which a company must disclose information that is 'reasonably likely' to have a material effect on financial condition, changes in financial condition or results of operations." While this is an improvement, there is still an ambiguity as to the dividing line between "reasonably likely" and "remote."

The SEC requires disclosure of enumerated items only "to the extent necessary to an understanding of the company's off-balance sheet arrangements and their effect on financial condition, changes in financial condition and results of operations." Specifically, the SEC requires a company to disclose

- "The nature and business purpose of the company's off-balance sheet arrangements;
- The significant terms and conditions of the arrangements;
- The nature and amount of the total assets and of the total obligations and liabilities of an unconsolidated entity that conducts off-balance sheet activities;
- The amounts of revenues, expenses and cash flows, the nature and amount of any retained interests, securities issued or other indebtedness incurred, or any other obligations or liabilities (including contingent obligations or liabilities) of the company

arising from the arrangements that are, or may become, material and the circumstances under which they could arise;

- Management's analysis of the material effects of the above items, including an analysis of the degree to which the company relies on off-balance sheet arrangements for its liquidity and capital resources or market risk or credit risk support or other benefits; and
- A reasonably likely termination or material reduction in the benefits of an off-balance sheet arrangement and any material effects."

The SEC specifies the need to account for "amounts of a company's known contractual obligations, aggregated by type of obligation and by time period in which payments are due." The SEC rejects requests to exclude "purchase orders and contracts for goods and services in the ordinary course of business." It requires "disclosure of the amounts of a company's purchase obligations without regard to whether notes, drafts, acceptances, bills of exchange, or other commercial instruments will be used to satisfy such obligations because those instruments could have a significant effect on the company's liquidity."

The SEC specifies that the categories of contractual obligations partly include

- Long-term debt obligations,
- Capital lease obligations,
- Operating lease obligations,
- Purchase obligations, and
- Other long-term liabilities reflected on the company's balance sheet under its Generally Accepted Accounting Principles (GAAP).

OBS ENTITIES[3]

In 2005, the SEC issued its "Report and Recommendations Pursuant to Section 401(c) of the Sarbanes-Oxley Act of 2002 On Arrangements with Off-Balance Sheet Implications, Special Purpose Entities, and Transparency of Filings by Issuers," which added much needed clarification and expanded examples for purchase orders, leases, derivatives, and contingent OBS obligations. The SEC's introduction underscores the complexity around OBS: "Issuers are involved in any number of contractual obligations, including debt obligations, retirement obligations, compensation agreements, leases, guarantees, derivatives, and obligations to purchase goods and services. In many cases, liabilities are recognized on the balance sheet at the inception of the contract, because one party has performed. For example, if an issuer borrows money, it recognizes a liability upon receipt of the funds. In other cases, liabilities are recognized as time passes, as in the case of interest related to the borrowed funds. In still other cases, contractual obligations remain off the balance sheet. Examples of these obligations may include operating leases, portions of obligations related to retirement plans, certain guarantees, and certain derivatives."

The 2005 SEC Report and Recommendations provide much needed additional background on OBS entities and obligations. The SEC's initial ruling was weak in providing examples and scenarios. "Companies have used off-balance-sheet entities responsibly and irresponsibly for some time. These separate legal entities were permissible under Generally Accepted Accounting Principles (GAAP) and tax laws so that companies could finance business ventures by transferring the risk of these ventures from the parent to the off-balance-sheet subsidiary. This was also helpful to investors who did not want to invest in these other ventures."

In a major understatement, the SEC noted in its 2005 Report that Enron and similar scandals have given OBS a bad reputation as something underhanded "or at least less than fully transparent. The insinuation is that something that should be on the balance sheet is not, and that the reporting issuer has designed the transaction or arrangement to produce that result. However, questions about whether items should be reflected on the balance sheet do not arise only when there is an attempt to deceive financial statement users."

The SEC defends OBS by noting that "many legitimate transactions generate such questions, and there are, of course, bounds as to what should be included on a balance sheet. It is this broader, more-inclusive question of the proper bounds of what should be included on the balance sheet" that are addressed in its 2005 Report. According to the SEC, the common characteristic of OBS is their creation of a condition "in which there may be a legal or economic nexus between the issuer and risks, rewards, rights or obligations not reflected (or not fully-reflected) on the balance sheet."