



Anne M. Marchetti

Parson Consulting

BEYOND Sarbanes- Oxley Compliance

Effective Enterprise Risk Management

BEYOND SARBANES-OXLEY COMPLIANCE

Effective Enterprise Risk Management

ANNE M. MARCHETTI



WILEY

John Wiley & Sons, Inc.

**BEYOND
SARBANES-OXLEY
COMPLIANCE**

BEYOND SARBANES-OXLEY COMPLIANCE

Effective Enterprise Risk Management

ANNE M. MARCHETTI



WILEY

John Wiley & Sons, Inc.

This book is printed on acid-free paper. ☺

Copyright © 2005 by John Wiley & Sons, 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.

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 www.wiley.com.

Library of Congress Cataloging-in-Publication Data:

ISBN-13 978-0-471-72626-5

ISBN-10 0-471-72626-5

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

To my parents

ACKNOWLEDGMENTS

I would like to express sincere appreciation to Kathleen Hajduk and Robert Grenhart for their valuable contributions.

PREFACE

Through my work with public and private entities of all sizes in developing Sarbanes-Oxley compliance programs, the question I receive most often is “Once you establish compliance with Section 404, what’s next?” This book guides corporate accounting and financial executives through the requirements and value-added activities in the post-initial compliance environment. It demonstrates how to monitor and maintain strong internal control systems within finance and accounting operations. In addition, it outlines how to leverage the knowledge harvested through regulatory compliance to improve financial management and make the organization more efficient. In this book, I also suggest new ideas on how to identify and mitigate threats to the financial control environment. My objective for this book is to show readers how to meet compliance requirements, as well as build on initial compliance activities to improve the financial management processes.

CONTENTS

Part One	Initial Compliance	1
1	Sarbanes-Oxley Act Overview	3
2	Overview of Sarbanes-Oxley Sections 302, 404, and 409	17
3	Determining Organizational Readiness	29
4	The “Path” to Compliance	41
Part Two	Ongoing Maintenance and Monitoring	69
5	Change Management	71
6	Ongoing Compliance Activities	91
7	Audit Function Considerations	117
8	Other Ongoing Compliance Issues	133
Part Three	Beyond Compliance	143
9	Process Improvement Considerations	145
10	International Financial Reporting Standards	155
11	Non-U.S.-Based Companies and Sarbanes-Oxley Compliance	167
12	Financial Services Compliance Initiatives	173
<i>Appendix A Sarbanes-Oxley Section 302</i>		<i>183</i>
<i>Appendix B Sarbanes-Oxley Section 404</i>		<i>185</i>
<i>Appendix C Sarbanes-Oxley Section 409</i>		<i>187</i>

Contents

<i>Appendix D</i>	<i>Evaluation Questions to Understand the Current State of Control Processes</i>	189
<i>Appendix E</i>	<i>Internal Control over Financial Reporting</i>	191
<i>Appendix F</i>	<i>Evaluating Control Deficiencies</i>	193
<i>Appendix G</i>	<i>Sample Documentation</i>	197
<i>Appendix H</i>	<i>AS2 Control Testing Provisions</i>	219
<i>Appendix I</i>	<i>Responsibilities of Internal Auditing</i>	241
<i>Appendix J</i>	<i>Actual Internal Control Disclosures</i>	245
Index		267

**BEYOND
SARBANES-OXLEY
COMPLIANCE**

PART ONE

INITIAL COMPLIANCE

SARBANES-OXLEY ACT OVERVIEW

Enron, Arthur Andersen, WorldCom, Tyco, Adelphia. These companies have become household names mostly because of their past display of corporate greed, fraud, and accounting improprieties. The offenses of these few organizations are not representative of the majority of more than 15,000 public companies in the United States, yet the results of their abuses are far reaching. When the details of corruption emerged, and stock prices and retirement savings plummeted, the American public became outraged and demanded reform. On July 30, the U.S. Congress answered this public outcry for change and enacted the Sarbanes-Oxley Act of 2002 (the “Act”).

The Act was signed into law to improve the accuracy and transparency of financial reports and corporate disclosures, as well as to reinforce the importance of corporate ethical standards. As a result, the Securities and Exchange Commission (SEC) issued rules outlining the provisions of the Act. In addition, the New York Stock Exchange (NYSE), the American Stock Exchange (Amex) and the over-the-counter Nasdaq Stock Market (Nasdaq), have all significantly modified the standards for listing stocks on their exchanges. Many view the Act’s provisions for internal controls over financial reporting (Section 404) and executive certifications (Section 302) as painful and costly to implement with little derived benefit. Others see the mandated changes as an opportunity to implement best business practices, drive greater performance, and boost investor confidence.

Initial Compliance

OVERVIEW OF THE ACT

The Act is the most significant legislation impacting the accounting profession since the Securities Acts of 1933 and 1934, which it amends. It addresses a wide range of matters relevant to publicly held issuers and their auditors, including auditor oversight and independence, corporate responsibility for financial reports, and enhanced financial disclosures. The Act is composed of 11 Titles as outlined below.

Title Summaries

Title 1. Public Company Accounting Oversight Board (PCAOB or “Board”)

The Act establishes the board as a private, nonprofit company funded by annual accounting support fees assessed to issuers¹ (as defined in Section 3 of the Securities Exchange Act of 1934 (15 U.S.C.78c)). The board’s duties include the mandatory registering of public accounting firms that prepare audit reports; establishing auditing, quality control, ethics, and independence standards relating to the preparation of audit reports; conducting inspections of registered public accounting firms; and enforcing compliance with the Act.

Title 2. Auditor Independence

Title 2 prohibits registered public accountants conducting an issuer’s financial statement audit from performing nonauditing services such as bookkeeping, the design and implementation of financial information systems, appraisals, valuations, fairness opinions, internal audit outsourcing, and management functions. All audit and nonaudit services require preapproval by the audit committee of the issuer. Additionally, there are provisions for audit partner rotation, specific reporting requirements by registered public accounting firms to the issuers’ audit committee, and an absolute prohibition of an audit firm providing audit services to clients for one year if the client has hired certain employees of the registered public accounting firm in key financial positions.

Title 3. Corporate Responsibility

This provision of the Act mandates the SEC to direct the national securities exchanges and national securities associations to prohibit the listing of

Sarbanes-Oxley Act Overview

any security of an issuer that is not in compliance with the following Act requirements:

- Existence of audit committee oversight of registered public accounting firm
- Board of directors/audit committee independence
- Procedures for receiving complaints concerning accounting or auditing matters and anonymous employee concerns relating to questionable accounting or auditing matters established by the audit committee
- Audit committee authority to engage independent counsel and other advisors
- Provision of appropriate funding, as determined by the audit committee, for payment to the registered public accounting firm and to advisors hired by the audit committee

Title 3 also requires chief executive officer (CEO) and chief financial officer (CFO) certifications of financial statements, outlines penalties for corporate officers and directors for material noncompliance, and prohibits insider trading during pension fund blackout periods.

Title 4. Enhanced Financial Disclosures

Title 4 outlines requirements to help assure the accuracy of financial statements and supporting financial disclosures. It requires reporting of material unconsolidated and off-balance sheet transactions as well as mandates that pro forma financial information is factual and complete, and reconciles with the financial condition and results of operations of the issuer. Personal loans to executives are prohibited; issuers are required to disclose whether or not they have a code of ethics for senior financial officers, and mandates that the audit committee include at least one financial expert as defined by the Act. This provision also outlines requirements regarding management's assessment of internal controls and the real-time disclosure of material changes to financial conditions or operations.

Title 5. Analyst Conflicts of Interest

This section of the Act requires the SEC, or national securities exchanges and national securities associations, to implement rules to improve "public confidence in securities research, and to protect the objectivity and independence of securities analysts"²

Initial Compliance

Title 6. Commission Resources and Authority

Pursuant to Title 6, \$98 million in funding is authorized to the SEC to hire an additional 200 professionals to provide enhanced oversight of auditors and audit services required by Federal securities laws.

Title 7. Studies and Reports

Title 7 authorizes the General Accounting Office (GAO) and the SEC to perform studies and issue reports investigating the consolidation of public accounting firms; the role of credit rating agencies in the securities market; the number of professionals found to have aided and abetted a violation of securities laws from the period January 1, 1998, to December 31, 2001; the enforcement actions taken by the Commission involving violations of reporting requirements; and whether investment banks and financial advisers assisted public companies in obfuscating their true financial condition.

Title 8. Corporate and Criminal Fraud Accountability

This provision of the Act, which is also referred to as the Corporate and Criminal Accountability Act of 2002, details the penalties for the destruction of corporate audit records and the willful destruction, alteration, or falsification of records in Federal investigations and bankruptcy proceedings. This section also establishes a five-year record retention period for audit or review workpapers and provides protection for whistleblowers.

Title 9. White-Collar Crime Penalty Enhancements

The Act in Title 9, which is also referred to as the White-Collar Crime Penalty Enhancement Act of 2002, modifies the Federal Sentencing Guidelines to increase the penalties for white-collar crimes. More importantly for issuers, it establishes a requirement for the CEO/CFO certification of periodic financial statements and specifies the penalties for the failure to certify and the willful certification of knowingly false financial reports. Penalties range from \$1 million to \$5 million and may include imprisonment for up to 20 years depending on the violation.

Title 10. Corporate Tax Returns

Title 10 simply states that “[I]t is the sense of the Senate that the Federal income tax return of a corporation should be signed by the CEO of such corporation.”³

Title 11. Corporate Fraud Accountability

The Corporate Fraud Accountability Act of 2002, or Title 11, provides for additional fines and penalties for individuals who fraudulently alter or destroy documents or impede an official proceeding.

Act Requirements

The requirements of the Act are intricate and complex and affect the entire organization regardless of the operational infrastructure. Exhibit 1.1 displays how the significant provisions of the Act influence specific aspects and individuals of a public company, including the relationship of the registered public auditor.

The provisions of the Act that address independence, officer codes of conduct, auditor oversight and hiring, audit approval, and prohibited services apply directly to the audit committee. Other provisions that deal with the forfeiture of incentive pay, the prohibition of personal loans, and whistleblower protection policies may be the responsibility of the human resources department, while provisions regarding interpretations as a matter of law, codes of ethics, and record retention policies are normally the responsibility of the general counsel. Although public company compliance with all aspects of the Act is required, this book focuses only on those aspects of compliance that directly impact financial managers: Sections 302, 404, and 409. Discussion of these sections is divided into three main parts: initial compliance, ongoing maintenance and monitoring, and beyond compliance.

Initial compliance provides an overview of the Act provisions for Sections 302, 404, and 409 and details suggested action steps necessary to comply with the requirements. This part also defines and contrasts the terms *reportable conditions*, *material weaknesses*, and *significant deficiencies* and provides practical examples of each.

Ongoing maintenance and monitoring details the responsibilities of the financial manager after initial compliance with the Act. Major subjects such as quarterly compliance processes, interfacing with both internal audit and registered public auditors, control testing, software considerations, and SAS 70 Letters are discussed in order to provide the financial manager with practical applications.

Beyond compliance addresses the opportunity to move Sarbanes-Oxley compliance from a routine checklist and one-time internal controls

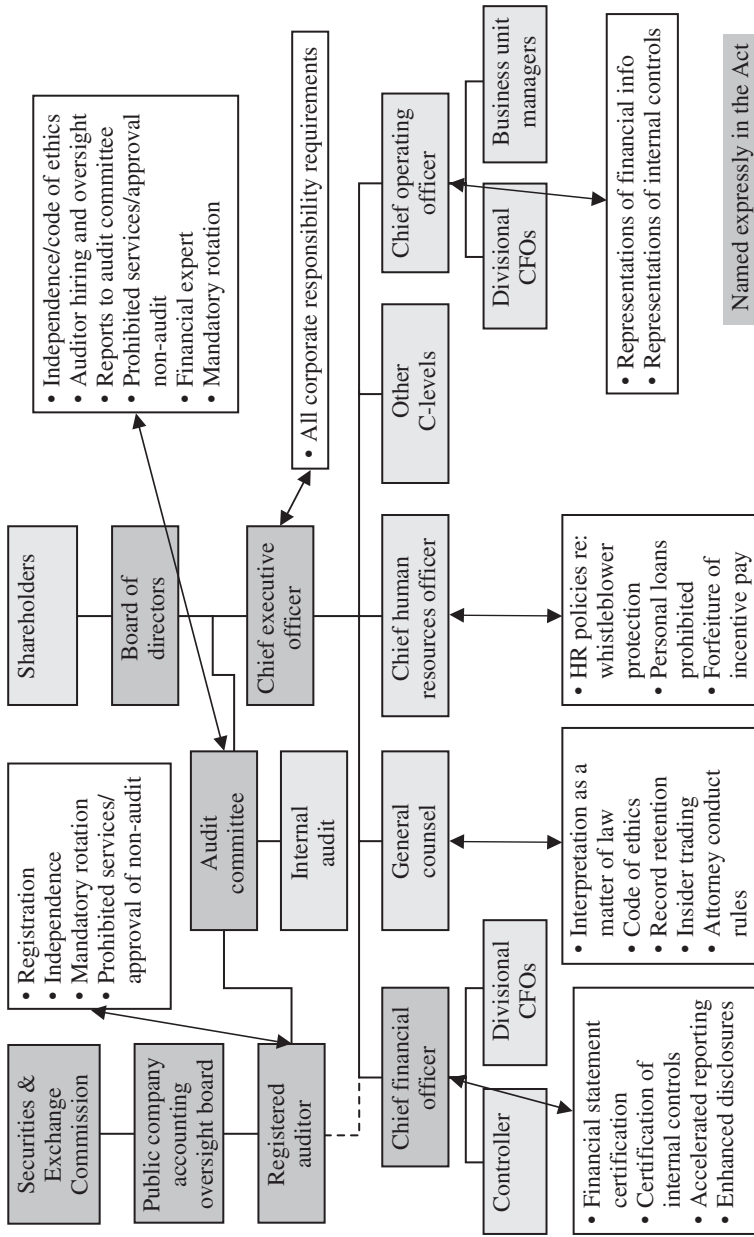


Exhibit 1.1 How Sarbanes-Oxley Affects Your Organization

Sarbanes-Oxley Act Overview

improvement process to a defining cultural change initiative. This Part addresses how the financial services industry may be affected by the ever-expanding local and global regulatory, compliance, and reporting requirements. The section concludes with a discussion on the implications for future European Union-listed companies with International Financial Reporting Standards (IFRS) and the differences that exist between IFRS and U.S. generally accepted accounting principles (GAAP).

INTERNAL CONTROLS ENVIRONMENT

Most companies would profess to have a strong emphasis on internal controls to ensure the reliability of financial reporting, yet in the absence of specific guidelines, determining the necessary level of control has primarily been a subjective decision. Early on, the impetus for effective internal controls was driven by the Securities Exchange Act of 1934, a law designed to restore investor confidence after the stock market crash of 1929, by providing more structure and government oversight. Issuers were later required to maintain adequate systems of internal controls after the Securities Exchange Act was amended in 1977. However, the term *adequate* was not clearly defined. In response to this requirement, most companies developed their own approach to compliance through the cooperative efforts of management, internal audit, and external auditors.

In the early 1990s, companies began adopting the Internal Controls–Integrated Framework of the Committee of Sponsoring Organizations (COSO) of the Treadway Commission’s study of internal controls.⁴ The COSO internal controls approach (Exhibit 1.2) is a framework designed to establish an internal control system for an entire company not limited to financial or financial reporting controls. This framework balances control objectives with the required control components necessary to maintain effective internal control within a company, process, or function. The three COSO control objectives are as follows: accurate and reliable financial reporting, effective and efficient operations, and compliance with laws and regulations. The COSO framework breaks effective internal control into five interrelated components:

1. Control environment
2. Risk assessment
3. Control activities

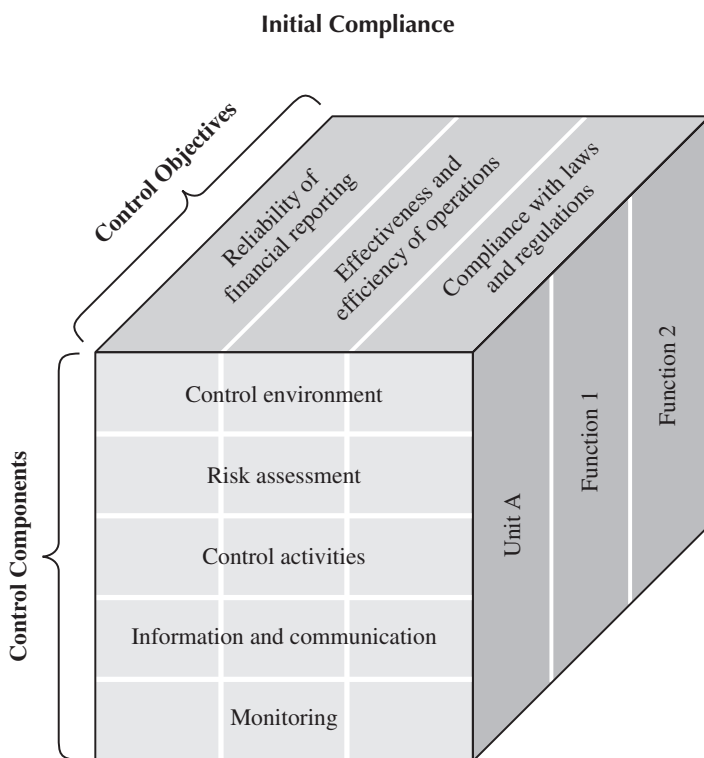


Exhibit 1.2 COSO Internal Controls Approach

4. Information and communication
5. Monitoring

The Act has placed significant responsibility on issuers for designing, implementing, and maintaining effective systems of internal controls to assure adequate financial reporting to the SEC and investors. Paragraph 13 of PCAOB Auditing Standard No. 2, *An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements*, sets forth the standards for registered public auditor attestation of issuers' internal controls as required in Section 404(b) of the Act. Standard No. 2 requires issuers to "base its assessment of the effectiveness of the company's internal control over financial reporting on a suitable, recognized control framework established by a body of experts that followed due-process procedures, including the broad distribution of the framework for public comment."⁵ Paragraph 13 concludes by mandating that an internal control assessment framework is suitable only when it:

Sarbanes-Oxley Act Overview

- Is free from bias
- Permits reasonably consistent qualitative and quantitative measurements of a company's internal control over financial reporting
- Is sufficiently complete so that those relevant factors that would alter a conclusion about the effectiveness of a company's internal control over financial reporting are not omitted
- Is relevant to an evaluation of internal control over financial reporting⁶

Additionally, Paragraph 13 states that the COSO integrated framework to internal controls “provides a suitable and available framework for purposes of management assessment” and “[f]or that reason, the performance and reporting directions in this standard are based on the COSO framework”⁷ even though other suitable standards may exist or may be developed in the future. The internal control delivery framework presented in Chapter 3 is based on the COSO Internal Control-Integrated Framework.

In addition to SEC- and COSO-driven internal control initiatives, many companies in specific industries such as pharmaceuticals and defense have historically placed a greater emphasis on internal controls because of specific regulatory requirements or other industry-specific environmental factors. These issuers may be in a better position than most issuers to more rapidly implement the requirements of the Act. They have already lived through a crisis similar to the one that prompted the Sarbanes-Oxley Act of 2002.

In the early and mid-1980s, the defense industry reeked of fraud, overcharges, and the perception of impropriety. In response to adverse headlines publicizing corruption, multiple congressional hearings, and the release of the Congressional report, *A Quest for Excellence*, the CEOs of 32 defense contractors met and established the Defense Industry Initiative on Business Ethics and Conduct (DII).⁸ The DII established six principles for doing business.

These principles, which establish a code of conduct or ethics, encourage internal reporting of violations of the code with the promise of no retaliation for such reporting. The principles also require the establishment of internal controls, a process for monitoring such controls, and a procedure for reporting violations. Defense contractors aggressively implement internal controls in part to protect themselves from the significant fines and penalties established for violating government contracting rules as well as fraud statutes and the Anti-Kickback Act of 1986. Most defense contractors incorporated the COSO framework into their internal control structures and

Initial Compliance

as a result may have a good basis from which to implement the additional provisions of the Act.

Like the crisis in the defense industry, the scandals leading to the passing of the Act resulted in a loss of confidence and faith in corporate leadership and the integrity of financial reporting. The perception is that boards of directors had simply become that of a “rubber stamp” approver of management decisions. In the minds of many investors, boards had forgotten their most important role: corporate oversight and governance.

The Act and the resultant changes—including SEC requirement and regulations, the formation of the PCAOB, and changes to listing requirements of the NYSE, Nasdaq, and Amex—have all forced businesses to reevaluate their organizational structure and systems of internal control. These changes have created new roles as well as modified existing roles for the individuals involved in the financial reporting process.

EFFECTS ON FINANCIAL REPORTING PROCESS PARTICIPANT HIERARCHY

Simply reading the Act provides enough information to know that corporate America must change the way it conducts business. The Act affects all of the participants in the financial reporting process from the users of the financial reports and information released by issuers to the individual employee who enters data to record a transaction. The following briefly outlines the effect the Act will likely have on each participant.

Investors and Other Users of Financial Data

Why did anyone care about the financial scandals and fraudulent activities involving companies such as Enron, WorldCom, and Adelphia? Simply stated, it is because the market values of those companies declined significantly when the magnitude of the fraud was realized. This resulted in investments and retirement savings losses of billions of dollars.

For investors and other users of financial data, the Act and other resultant regulatory changes strengthen the controls over financial reporting by requiring issuers to ensure timely, accurate, and complete financial reporting and real-time disclosure of financial information. To encourage issuers to comply with the new requirements, the Act specifically imposes signif-

Sarbanes-Oxley Act Overview

ificant criminal penalties and fines for corporate executives. Will these rules prevent all future corporate scandals? Probably not, but they will likely be enough incentive to improve the quality, accuracy, and timeliness of financial data to allow investors to make informed decisions regarding their investments.

Regulatory Bodies

The Act resulted in several important changes to regulatory bodies. First, the Act mandated the creation of the PCAOB to oversee the public accounting industry and to set standards for conducting the review of issuer's internal control over financial reporting. Second, the Act effected several changes to SEC reporting requirements, including provisions for mandatory real-time disclosures of certain changes to issuers' financial conditions and new accelerated due dates for quarterly and year-end reports. Finally, the Act required the national securities exchanges to change their listing requirements for issuers subject to the Act.

The Board of Directors

The two primary responsibilities given to boards of directors are (1) strategic direction and leadership of the business, and (2) corporate oversight. The Act and changes made by the national listing exchanges reinforce those responsibilities and ensure they are taken seriously. These changes require boards to be composed of a majority of independent members, hold meetings with only independent directors, and implement corporate governance and codes of ethics.

Audit Committee

The role of the audit committee has also changed. First, the audit committee must consist of only independent directors, and the board must disclose if the audit committee does not contain at least one "financial expert" as defined by the SEC. Second, the audit committee is solely responsible for the engagement and compensation of the external auditor and oversight of the auditors work relating to the audit of financial statements. Finally, the

Initial Compliance

external auditor now reports directly to the audit committee and no additional services can be provided without the committee's preapproval.

External Auditors

In addition to now reporting directly to the audit committee, external auditors must register with the PCAOB, refrain from performing certain nonauditing services, and must comply with audit partner rotation requirements. The external auditor is also responsible for an attestation review of the issuer's internal control over financial reporting and report on management's assessment of the same.

Executive Management

Executive management is now explicitly responsible for establishing and maintaining a system of internal control over financial reporting and creating an annual assessment of the same. The CEO and CFO are responsible for the financial reports filed with the SEC and must certify the accuracy of such reports under the risk of criminal penalties and fines. Other members of the executive management team are responsible for the new requirements relating to codes of ethics, record retention, insider trading, attorney conduct rules, whistleblower policies, as well as other legal and human resource issues.

Management and Staff

While the Act does not specifically mention any requirements of managers and supporting staff, these individuals will likely be directly responsible for the majority of the additional work that will be required to comply. Since executive management is held accountable for compliance, it is in their best interest to ensure their financial managers are knowledgeable about the Act and its impact on their company.

Based on the work effort outlined, it is clear that companies will experience significant increases in costs and time necessary to comply with the provisions of the Act and the related regulatory changes. These increased costs will be related to:

Sarbanes-Oxley Act Overview

- More frequent board and audit committee meetings
- Increased oversight activities
- Continual communication with external auditors
- Increased legal and human resource work resulting from new policies and procedures

By far, the most significant cost increases will result from the external auditor attestation of internal control over financial reporting and the internal cost of complying with the provisions of Section 302, Section 404, and Section 409 of the Act.

The cost of compliance will vary based on the size of the company, the number of operations, and the complexity of the business. Nonetheless the total is still significant for most organizations. A January 2004 Financial Executives International (FEI) survey suggests that Section 404 compliance will cost companies, on average, 12,265 internal people hours, 3,059 external resource hours to supplement internal hours, \$732,100 for external consulting, and \$590,100 for the external auditors attestation review.⁹ To determine a reasonable estimate of the cost of compliance, companies will first need to understand the requirements of the Act and what efforts will be needed to comply. The next three chapters discuss the specific requirements of Section 302, Section 404, and Section 409, respectively.

A RESOURCE FOR FINANCIAL MANAGERS

This book is intended to help financial managers go beyond mere compliance and seize the opportunity to improve business practices and/or processes, drive greater performance, and transform the perception of the finance organization into that of a value-added key contributor to the company. For discussion purposes, *financial manager* refers to anyone who is a CFO, controller, vice president of finance, divisional CFO, or a manager who directly works for someone in such a position.

This book focuses on the aspects of Sarbanes-Oxley that impact those employees working directly or indirectly for the CFO. It is designed to lead the reader from initial compliance with the Act, through ongoing maintenance and monitoring, and ultimately to beyond compliance; however, each section can be read and applied individually.

Initial Compliance

The PCAOB's web site (www.pcaob.com) is a perfect complement to the information contained in this book. The web site lists the board's current and pending regulatory actions regarding rules and the adoption of auditing standards. The site also maintains briefing papers and other documents that can serve as valuable information for financial managers who are responsible for implementing various sections of the Act, as well as Q&A documents clarifying opinions on issues related to the implementation of the standards of the PCAOB.¹⁰

NOTES

1. The term *issuer* means an issuer (as defined in Section 3 of the Securities Exchange Act of 1934, the securities of which are registered under Section 12 of that Act or that is required to file reports under section 15(d) of that Act, or that files or has filed a registration statement with the Securities and Exchange Commission that has not yet become effective under the Securities Act of 1933, and that has not withdrawn).
2. The Act, Title 5, Section 501.
3. The Act, Title 10, Section 1001.
4. Internal Controls—Integrated Framework. The Committee of Sponsoring Organizations of the Treadway Commission, "Struggling to incorporate the COSO recommendations into your audit process?" www.coso.org.
5. PCAOB Auditing Standard No. 2. An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements was approved by the SEC June 18, 2004, Paragraph 13.
6. *Id.*
7. PCAOB Auditing Standard No. 2. An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements was approved by the SEC June 18, 2004, Paragraph 14.
8. Defense Industry Initiative, www.dii.org.
9. FEI Survey on Sarbanes-Oxley Section 404 Implementation January 2004 available on the FEI web site at www.fei.org.
10. PCAOB Staff Questions and Answers Auditing Internal Controls over Financial Statements, June 23, 2004, page 1.

OVERVIEW OF SARBANES-OXLEY SECTIONS 302, 404, AND 409

SECTION 302

The Sarbanes-Oxley Act of 2002 has literally rewritten the rules for corporate governance, disclosure, and reporting. It has fundamentally changed the business and regulatory environment, leaving public companies with the demanding task of modifying their operations in order to comply.

Exhibit 2.1 outlines the key requirements of the Act, notes which departments within the corporation are affected, and displays the key compliance focus for the financial manager: Section 302 financial statement certification, Section 404 certification of internal controls, and Section 409 real-time disclosures of changes to reported information.

Section 302 requires chief executive officers (CEOs) and chief financial officers (CFOs) of companies filing reports pursuant to the provisions of the Securities Exchange Act of 1934 (15 USC 78m, 78o(d)) to submit a certification with the submission of the required reports (see Appendix A). The Act is silent as to whether the certification is a joint certification or whether each applicable company officer is required to certify individually. However, completing separate certifications, while not limiting the company's liability for false certifications, would shield separate officers from improper certifications of other officers.

The Section 302 certification consists of six specific certification points:

1. "[T]he signing officer has reviewed the report."¹ Reviewing the report is not the same as reading the report. Simply reading the report does not meet the intention of the Act—holding corporations

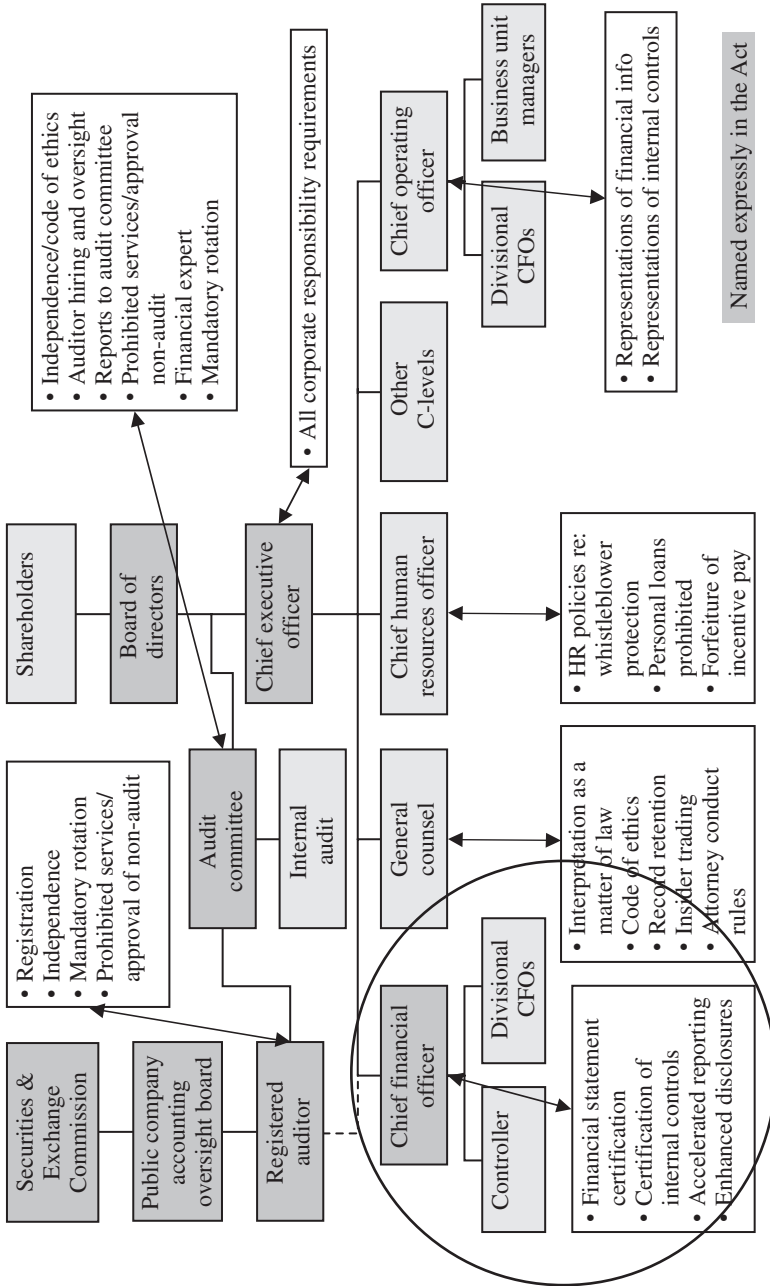


Exhibit 2.1 Who Is Impacted?

Overview of Sarbanes-Oxley Sections 302, 404, and 409

and their officers responsible for the content and accuracy of financial reports. Corporate officers must apply appropriate levels of scrutiny in order that they understand the material, sources, key assumptions, and estimates included in financial reports.

2. “[B]ased on the officer’s knowledge, the report does not contain any untrue statement of a material fact or omit to state a material fact necessary in order to make the statements made, in light of the circumstances under which such statements were made, not misleading.”² In other words, based on the officer’s knowledge, the report must be accurate and complete. Accurate in that it is factual or not containing any “untrue statement of material fact.”³ Complete in that it contains all relevant data so as to accurately present information and not mislead the reader.

An important aspect of this provision is the phrase “based on the officer’s knowledge.” Board interpretation of this phrase has yet to be determined, but applying a legal “reasonableness” test is appropriate. While the CFO of a large corporation may not be expected to know the details of the accounts payable balance at each operating division, it would not be reasonable for the CFO to certify a financial report knowing that one division’s accounts payable balance was disproportionately high for its size and nature. The CFO in this case should reasonably know that the accounts payable data may be inaccurate and delay certifying until the data are verified as accurate.

3. “[B]ased on such officer’s knowledge, the financial statements, and other financial information included in the report, fairly present in all material respects the financial condition and results of operations of the issuer as of, and for, the periods presented in the report.”⁴ In addition to the financial statements and information being accurate and complete, they must correctly represent the results of operations for the specific period presented in the report. As discussed in point 2, the officer’s knowledge and understanding of financial operations must be sufficient enough to apply a reasonableness test to the report. Ultimately, the signing officers must be comfortable with the content, accuracy, and completeness of financial reports, as well as such reports’ conformity with generally accepted accounting principles (GAAP).

Initial Compliance

4. “[T]he signing officers

- are responsible for establishing and maintaining internal controls;
- have designed such internal controls to ensure that material information to the issuer and its consolidated subsidiaries is made to such officers by others within those entities, particularly during the period in which the periodic reports are being prepared;
- have evaluated the effectiveness of the issuer’s internal controls as of a date within 90 days prior to the report; and
- have presented in the report their conclusions about the effectiveness of their internal controls based on their evaluation as of that date.”⁵

Certifying officers are ultimately responsible for the design, implementation, effectiveness, continuing operation, and evaluation of all internal controls that ensure accurate and complete disclosure of financial reports. A critical component of the internal control environment is ensuring that the appropriate level of information effectively flows through the organization to the certifying officers. This process should seek to prevent information from becoming distorted, clouded, or blocked altogether.

5. “[T]he signing officers have disclosed to the issuer’s auditors and the audit committee of the board of directors (or persons fulfilling that equivalent function):

- all significant deficiencies in the design or operation of internal controls that could adversely affect the issuer’s ability to record, process, summarize, and report financial data and have identified for the issuer’s auditors any material weaknesses in internal controls; and
- any fraud, whether or not material, that involves management or other employees who have a significant role in the issuer’s internal control.”⁶

In addition to detailing the effectiveness of internal controls over financial reporting, the certifying officers must also disclose all “significant deficiencies” and incidences of management fraud discovered to the issuer’s audit committee (or equivalent function as defined in the Act) and the issuer’s registered public auditor. Fraud reporting is limited to situations involving management

Overview of Sarbanes-Oxley Sections 302, 404, and 409

employees who, by nature of their position, play a substantive role in the issuer's internal controls. Fraud reporting is required regardless of the materiality of the fraudulent action. Fraudulent activities, in and of themselves, require timely disclosure.

6. "[T]he signing officers have indicated in the report whether or not there were significant changes in internal controls or in other factors that could significantly affect internal controls subsequent to the date of their evaluation, including any corrective actions with regard to significant deficiencies and material weaknesses."⁷ The signing officers must further certify that their financial reports include disclosure, both affirmative and negative, and whether there were any changes to internal controls after the completion of the evaluation that could have a significant impact on internal controls. Such disclosures should also include all "other factors" that could affect internal controls. While the Act does not define "other factors," it is likely that it is intentionally broad so it would encompass any internal change or external factor that could impact internal controls.

Examples of internal changes may include adjustments in accounting practices, implementation of new software systems, and restructuring activities. Examples of external factors include regulatory changes such as the Act, natural disasters, or acquisitions. While most of these examples represent operational changes, they all could potentially result in an immediate and permanent change to the internal control environment and thus, affect financial reporting.

The Securities and Exchange Commission (SEC) approved rules for Section 302(a) of the Act requiring an issuer's CEO and CFO to certify each quarterly and annual report for all periods ending after August 29, 2002. Section 302 certification requirements do not allow for a single review of internal controls that officers can rely on for future certifications. Section 302 requires a new officer certification with each quarterly and annual periodic reports. Issuers must not only assess their current state, but also seek to enhance internal control processes and implement monitoring and testing systems to assure the integrity of future certifications. Unlike Section 404, Section 302 of the Act does not require registered public accounting firm attestation of the internal control process. Many issuers are electing to ultimately integrate their Section 302 and 404 compliance efforts in order to have a unified and streamlined approach to their internal control frameworks and the related certifications.

SECTION 404

Section 404, Management Assessment of Internal Controls (see Appendix B), is the section of the Act that often presents the greatest challenge and the most work for finance managers. It requires the SEC to promulgate rules mandating that all annual reports pursuant to sections 13(a) or 15(d) of the Securities Exchange Act of 1934 (i.e., Annual Report, Forms 10-K, 10-KSB, 20-F, and 40-F) include management's assessment of the integrity of internal control over financial reporting as of the end of the issuer's fiscal year for which they are reporting. As prescribed in Section 404, the management assessment of internal control over the financial reporting process applies to all issuers except for investment companies registered under Section 8 of the Investment Company Act of 1940 (15 U.S.C. 80a–8).

The Act states that management is responsible for “establishing and maintaining an adequate internal control structure and procedures for financial reporting”⁸ as well making an assessment “of the effectiveness of the internal control structure and procedures of the issuer for financial reporting”⁹ as of the end of the fiscal year for which the issuer is reporting. The Act further requires that a “registered public accounting firm that prepares or issues the audit report for the issuer shall attest to, and report on, the assessment made by the management of the issuer” and that such “attestation made under this subsection shall be made in accordance with standards for attestation engagements issued or adopted by the Board. Any such attestation shall not be the subject of a separate engagement.”¹⁰

Section 404 requires more than Section 302 compliance by requiring the issuer's registered public accounting firm to attest to and report on management's assessment as part of the annual financial statement audit engagement. Public Company Accounting Oversight Board (PCAOB) Auditing Standard No. 2, *An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements*,¹¹ became effective June 17, 2004, and sets the standard for internal control attestation engagements. Auditing Standard No. 2 details both the work required to audit and attest to the internal controls over financial reporting and the interrelationship of the attestation audit to the annual audit of financial statements.

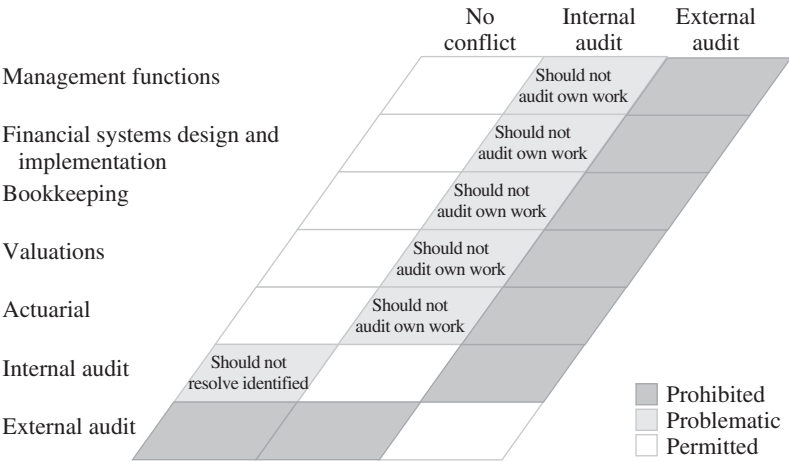
The bulk of internal control compliance work is typically the primary responsibility of financial managers in conjunction with support from other functional personnel. In the past, financial managers would often engage their outside public accounting firm and the services of their internal auditors to assist with the design, implementation, and assessments of

Overview of Sarbanes-Oxley Sections 302, 404, and 409

internal control processes. However, Section 103(b) of the Act and revised SEC rules redefine auditor independence.

Pursuant to Section 103(b) rules, auditors cannot function in the role of management, cannot audit their own work, and cannot serve in an advocacy role for their client. The responsibility of ensuring auditor independence lies with the issuer, not the auditors. The auditor can no longer identify control deficiencies, design and recommend specific corrective action, and assist issuers with implementation. Issuers will either have to perform all of this work with internal resources or seek assistance from “no conflict resources” (external resources who are not registered public accounting firms or external auditors other than the registered public accounting firm performing the issuer’s annual audit).

Exhibit 2.2 highlights specific services that are prohibited, permitted, or problematic for external auditors and no-conflict resources. It also outlines the role of the internal audit department, which can be problematic for issuers since auditors should not examine their own work. As a result, many companies are limiting the role of internal audit in the internal controls program.



Principles of Independence:

In fact and appearance, an auditor cannot:

- Function in the role of management
- Audit his or her own work
- Serve in an advocacy role for a client

Therefore, ensuring independence lies with the company, not the auditor.

Exhibit 2.2 Independence Standards: Who Does What?

SECTION 409

Section 409, Real Time Issuer Disclosures, requires all public companies to disclose important corporate events in a timely manner. Specifically, Section 409 stipulates “[e]ach issuer reporting under section 13(a) or 15(d) [of the Securities Exchange Act of 1934] shall disclose to the public on a rapid and current basis such additional information concerning material changes in the financial condition or operations of the issuer, in plain English, which may include trend and qualitative information and graphic presentations, as the Commission determines, by rule, is necessary or useful for the protection of investors and in the public interest.”¹² The full text of Section 409 is shown in Appendix C.

In instituting this provision, the SEC expanded the disclosure requirements of events that are reportable on Form 8-K pursuant to the Securities Exchange Act of 1934.¹³ The SEC had originally proposed amending Form 8-K reporting requirements in June of 2002¹⁴ prior to Congress enacting the Sarbanes-Oxley Act. As a result of Section 9 of the Act, the SEC revised its June 2002 proposal, reviewed comment letters received concerning the proposed rules, and ultimately issued final rules,¹⁵ which the SEC believes are responsive to Congress’s intent in the Act. In addition to meeting the requirements of the Act, the SEC believes that the final rule as adopted “will benefit markets by increasing the number of unquestionably or presumptively material events that must be disclosed currently. They will also provide investors with better and more timely disclosure of important corporate events.”¹⁶

The SEC final rule amended the existing disclosure provisions, which required a disclosure of nine specific events. Under the old Form 8-K rules, issuers were only required to make accelerated disclosures after the occurrence of nine specific events and were able to delay disclosure of other significant events until the next required reporting date. This delayed reporting is specifically addressed in section 409 of the Act. The new final rule expands disclosure to include eight new disclosable events, transfers two events from periodic reports, and broadens the scope of two existing events. Also included in the list of specifically required disclosable events are three items carried over from Form 8-K Regulation FD disclosures, disclosure of other events, and financial statement and exhibits. A listing of Form 8-K and Section 409 disclosure events is provided in Exhibit 2.3.

In the final rule, the SEC also changed the timing of disclosures. If an issuer experiences any of the 22 triggering events, disclosure is required by

Section 1. Registrant's Business and Operations	
Item 1.01	Entry into a material definitive agreement
Item 1.02	Termination of a material definitive agreement
Item 1.03	Bankruptcy or receivership
Section 2. Financial Information	
Item 2.01	Completion of acquisition or disposition of assets
Item 2.02	Results of operations and financial condition
Item 2.03	Creation of a direct financial obligation or an obligation under an off-balance sheet arrangement of a registrant
Item 2.04	Triggering events that accelerate or increase a direct financial obligation or an obligation under an off-balance sheet arrangement
Item 2.05	Costs associated with exit or disposal activities
Item 2.06	Material impairments
Section 3. Securities and Trading Markets	
Item 3.01	Notice of delisting or failure to satisfy a continued listing rule or standard; transfer of listing
Item 3.02	Unregistered sales of equity securities
Item 3.03	Material modifications to rights of security holders
Section 4. Matters Related to Accountants and Financial Statements	
Item 4.01	Changes in registrant's certifying accountant
Item 4.02	Nonreliance on previously issued financial statements or a related audit report or completed interim review
Section 5. Corporate Governance and Management	
Item 5.01	Changes in control of registrant
Item 5.02	Departure of directors or principal officers; election of directors; appointment of principal officers
Item 5.03	Amendments to articles of incorporation or bylaws; change in fiscal year
Item 5.04	Temporary suspension of trading under registrant's employee benefit plans
Item 5.05	Amendments to the registrant's code of ethics, or waiver of a provision of the code of ethics
Section 6. [Reserved]	
Section 7. Regulation FD	
Item 7.01	Regulation FD disclosure
Section 8. Other Events	
Item 8.01	Other events
Section 9. Financial Statements and Exhibits	
Item 9.01	Financial statements and exhibits

Exhibit 2.3 Form 8-K and Section 409 Disclosure Triggering Events

Initial Compliance

the end of the fourth business day following the date of occurrence. For example, if an issuer completes an acquisition of a business on Monday, it would have until the end of business on Friday to disclose this information via Form 8-K. This is a change from the previous five business day or 15 calendar day reporting requirement.

The Commission believes that requiring accelerated disclosure for the 22 events and shortening the deadline for disclosure will “benefit markets by increasing the number of unquestionably or presumptively material events that must be disclosed currently” and “also provide investors with better and more timely disclosure of important corporate events.”¹⁷ The commission also does not believe that the four business day reporting deadline will be problematic or significantly increase the cost of reporting. SEC data suggest that of the approximately 68,000 Form 8-K reports they sampled, in excess of 74% were filed within four business days of the reported event triggering date.¹⁸ While the SEC acknowledges that their less than scientific study did not verify the accuracy of the reported event triggering dates,¹⁹ the high percentage of reports filed within four business days is nevertheless significant enough to conclude that the four business day reporting requirement does not place a significant burden on public companies.

In order to comply with Section 409 of the Act and the new accelerated Form 8-K disclosure requirements, financial managers must become familiar with the SEC’s specific disclosure events requirements.

NOTES

1. The Sarbanes-Oxley Act, Title 3, Section 302.
2. *Id.*
3. *Id.*
4. *Id.*
5. *Id.*
6. *Id.*
7. *Id.*
8. Sarbanes-Oxley Act Section 404 (a)(1).
9. Sarbanes-Oxley Act Section 404 (a)(2).
10. Sarbanes-Oxley Act Section 404 (b).
11. Effective pursuant to SEC Release No. 34-49884; File No. PCAOB-2004-03, June 17, 2004.

Overview of Sarbanes-Oxley Sections 302, 404, and 409

12. Sarbanes-Oxley Act Section 409.
13. Securities Exchange Act of 1934 17 CFR 249.308.
14. SEC Release No. 33-8106 (June 17, 2002) [67 FR 42914].
15. SEC Release No. 33-8400, Additional Form 8-K Disclosure Requirements and Acceleration of Filing Date (March 16, 2004).
16. Federal Register Page 15595, Volume 69, No. 58, March 25, 2004, Rules and Regulations.
17. Federal Register Page 15595, Volume 69, No. 58, March 25, 2004, Rules and Regulations.
18. Federal Register Page 15611, Volume 69, No. 58, March 25, 2004, Rules and Regulations.
19. *Id.*

3

DETERMINING ORGANIZATIONAL READINESS

Sarbanes-Oxley has fundamentally changed the way corporations conduct business. Organizations must recognize that they now operate in an environment that demands accountability and a greater focus on financial controls. The requirements of the Act are a matter of law and dictate how corporations, executive officers, and financial managers must run their businesses as well as how professional accounting firms must conduct audits of financial controls over financial reporting. In addition to creating provisions for executive officer certifications of financial statements and certification of the internal controls over financial reporting, the Act created the Public Company Accounting Oversight Board (PCAOB), which has, among other duties, the responsibility of establishing auditing, quality control, and independence standards and rules. At the time of this publication, the PCAOB has issued three auditing standards and numerous briefing papers (see Exhibit 3.1) that are available on the PCAOB web site (www.pcaobus.org). These should be reviewed and fully understood by all financial managers with Section 302, 404, and 409 compliance responsibilities.

Auditing Standard No. 1. References in Auditor's Reports to the Standards of the Public Company Accounting Oversight Board

Auditing Standard No. 2. An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements

Auditing Standard No. 3. Audit Documentation

Exhibit 3.1 Public Company Accounting Oversight Board Auditing Standards

Initial Compliance

The success of a compliance initiative is greatly dependent on the tone set by the board of directors and executive officers, existing processes, environmental factors, and an organization's compliance approach. Does senior management view Act compliance as an overly burdensome cost of doing business or as an opportunity to change the corporate culture? Do they believe compliance will create more paperwork and less "real" business or do they believe that enhancing the control environment can drive productivity improvements and create competitive advantages? In a January 2004 PricewaterhouseCoopers survey of major corporation Sarbanes-Oxley Section 404 project leaders, only 7% of respondents reported that senior management views the cost of compliance with the Act as "[a]n unnecessary burden," while 52% believe it is a necessary cost of business and 41% believe it will actually improve their competitive positions.¹

THE REAL COST OF COMPLIANCE

Regardless of a company's position on the Act, the cost of compliance is real. A January 2004 Financial Executives International (FEI) survey on Act implementation efforts suggests that companies expect to invest significant employee time to simply comply with Section 404 requirements.² Survey results show that respondents expect to spend an average of 12,265 internal hours on Section 404 compliance alone.³ For companies with annual revenues of less than \$25 million, additional internal hours invested to achieve compliance drops to an average of 1,150.⁴ For companies with annual revenues of more than \$5 billion, average internal hours grow to 35,000 or the equivalent of about 18 full-time employees for a year.⁵ These survey data only reflect compliance with Section 404 and use of internal resources. In the same survey, respondents indicated that they expect to incur on average an additional \$732,100 for external consulting, software, and other vendor charges.⁶ Companies with less than \$25 million in annual revenues expect to incur \$170,000 of such expenses, while companies with more than \$5 billion in annual revenues expect to incur \$1,390,100 of such expenses.⁷

The results of a January 2004 PricewaterhouseCoopers survey support the findings of the FEI survey. Almost 73% of respondents to the PricewaterhouseCoopers survey have significantly increased the level of effort needed to comply with Section 404 over their original estimates. Within that 73% of respondents who reported a significant increase in their original time estimates:

Determining Organizational Readiness

- 33% increased their efforts about 25%.
- 37% increased their efforts about 50%.
- 10% increased their efforts about 75%.
- 5% increased their efforts about 100%.
- 15% increased their efforts more than 100%.

An astounding 67% of respondents have more than doubled their initial time estimates. The scope of these surveys specifically excludes the time and related expense for the required registered public accounting firm attestation. This attestation could cost on average an additional \$590,100 in annual fees (\$52,200 for companies with annual revenue less than \$25 million and \$1,531,400 for companies with more than \$5 billion in annual revenue).⁸

DEFINING THE SCOPE OF YOUR COMPLIANCE PROGRAM

There are many different approaches to Sections 302, 404, and 409 compliance. The method advocated in this book is an integration of all three sections into a single unified approach. By implementing a vigorous and thorough Section 404 compliance process that includes periodic testing and monitoring, issuers should also be able to more efficiently comply with the requirements of Section 302. The compliance approach described in this chapter can be individually applied to Section 302 and Section 404, but a unified approach will ultimately be more cost effective and efficient for continuous compliance with the Act. The results of a Parson Consulting survey completed in March 2004 seem to indicate that most companies are indeed buying into a unified approach. According to the survey, only 11.5% of companies plan on implementing Section 302 and Section 404 compliance efforts as completely separate activities.⁹

When issuers implement an effective and efficient Section 302 and 404 internal control framework that is attested by their registered public accounting firm, Section 409 compliance will typically exist. The data necessary for Section 409 real-time disclosure will flow directly from the internal control process to the appropriate employees for Form 8-K disclosure. What may be missing from the process, and should be addressed, is a control to ensure that employees responsible for Form 8-K disclosures are thoroughly trained and informed of the triggering events and the instructions necessary to complete a Form 8-K disclosure.

Initial Compliance

Additionally, a decision should be made early in the compliance implementation planning process whether the scope of compliance will be narrow, broad, or optimal. The narrow-scoped approach focuses primarily on financial reporting processes, specifically policies, procedures, processes, systems, and controls directly impacting the financial reporting process and the reliability of financial statements. This approach excludes from consideration all operational processes, operating improvements, and efficiencies.

The broad-scoped approach is a middle-of-the-road perspective between the narrow and optimal approaches. The broad-scoped approach focuses on policies, procedures, processes, systems, and controls that may materially impact the financial reporting process or the reliability of financial statements. This approach includes some operational processes, but excludes operating improvements and efficiencies.

Finally, the optimally scoped approach to compliance is based on a broader perspective that encompasses the review of financial reporting processes and operational processes throughout the enterprise. Companies that adopt this approach are effectively using the Act as a catalyst for cultural change throughout their organizations. They will not only review the adequacy of internal control over the financial reporting processes and all material operational processes, but will also set out to strengthen their systems of internal control enterprisewide, implement process improvements and efficiencies, as well as establish a comprehensive ongoing monitoring and continuous improvement process.

There is not only one answer to determining the scope of the compliance effort. Much will depend on the existing cultural climate and other factors such as time, cost, resource availability, and skill set, as well as the extent of existing internal controls. Many companies that are in highly regulated industries may feel they already have strong systems of internal controls that only need additional detailed documentation in order to meet the requirements of the Act. Additionally, companies effectively utilizing process improvement/quality control initiatives such as balanced scorecard, six sigma, and continuous process improvement teams may already be reaping significant productivity, efficiency, and competitive advantages, and may not see a favorable cost/benefit outcome in implementing an optimally scoped compliance approach.

A March 2004 survey by Parson Consulting examined the various approaches that companies are adopting to address the increased time and resource demands of their compliance programs. Roughly 35% of respon-

Determining Organizational Readiness

dents said they would implement a narrow-scoped approach to compliance, 30% would implement a broad-scoped approach, and 35% would implement an optimally scoped approach.¹⁰ When these data are split between large companies (those with market capitalization of \$1 billion or more) and smaller companies (those with market capitalization between \$75 million and \$1 billion) the results show that 47% of large companies take a narrow-scoped approach while only 27% of smaller companies take the same approach.¹¹ As stated above, this may be the result of the use of other broad-based process improvement initiatives or simply due to the perceived increased time and expense necessary to implement additional process improvement initiatives and internal control reviews across a large and complex enterprise.

CONSIDERATIONS PRIOR TO COMPLIANCE IMPLEMENTATION

Before beginning the compliance process for Sections 302, 404, and 409, financial managers should consider the current company environment. The following list of nine questions, while not 100% applicable to all companies, provides a basis for evaluating the current state of a business. The list provides a starting point for financial managers to form a foundation for the development and implementation of an effective compliance process. A summary of these questions appears in Appendix D.

1. *Are your accounting policies, practices, and procedures adequately documented, communicated, and understood throughout your organization?* Effective, easily assessable, and well-distributed written policies, practices, and procedures are one of the cornerstones to Act compliance. Such documents should be available to all employees within the organization, preferably in an electronic read-only format with restricted editing capabilities. Electronic documents promote timely, thorough, and accurate communication, which is vital in today's fast-paced, decentralized corporate environment.

Other considerations include the level and extent of existing documentation. Does the documentation include only narrative descriptions of policies, procedures, and internal controls for a specific process or does the documentation include flowcharts? Internal and external auditors have historically included flowcharts when reviewing a process and its related internal controls,

Initial Compliance

considering them a key component of adequate process and control documentation.

2. *Is your accounting staff sufficiently trained in generally accepted accounting principles (GAAP) and financial disclosure requirements?* Corporations often promote people into positions only to later learn that they are not adequately skilled or trained in the technical aspects required for the position. If key individuals do not currently have the skills to adequately perform their jobs, the organization is at risk. Key employees should be thoroughly versed in GAAP, Securities and Exchange Commission (SEC) reporting and disclosure requirements, as well as PCAOB auditing standards and rules that are appropriate to individual job requirements.
3. *Is your internal control system adequate to detect and report errors or fraud?* This is a key aspect of Act compliance and addresses the issues that led to the creation of the Act in the first place. Adequate internal control systems should be sufficient to prevent and detect errors and fraud. Companies with strong existing internal control infrastructures will likely require less additional work to comply with the Act than those companies with weak internal control structures.
4. *Is your internal audit activity sufficiently independent to report errors or deviations from GAAP and approved procedures?* Companies should consider applying the SEC auditor independence requirements to their internal audit functions. Application of these provisions will help to ensure that internal auditors are sufficiently independent. Requiring the internal audit department to report directly to the board of directors (instead of the chief financial officer or chief counsel); restricting auditors from performing work in divisions or departments where they have previously worked or will soon be working; and prohibiting audit managers from managing work within specific departments or divisions for extended periods will help to ensure the independence of the internal audit department. In addition, the role of the internal audit department must be closely monitored to ensure the group does not audit their own work.
5. *If your organization has multiple accounting locations, what procedures have you established to ensure that all locations are consistently following company policies, practices, and financial*

Determining Organizational Readiness

reporting procedures? Are policies, practices, and procedures consistent across all divisions? Are acquisitions required to change their historical policies, practices, and procedures to those of the parent corporation? Does the business have a documented consolidation reporting system and process? Organizations with multiple operating systems; inconsistent policies, procedures, practices, and internal controls; and nonintegrated consolidation systems inherently have a high level of risk that must be mitigated.

6. *Is your audit committee actively involved in the review of your financial reporting to shareholders?* Do you have a process in place that facilitates an open and collaborative relationship with the audit committee? The Act mandates that boards of directors and specifically, audit committees take a more active role in the oversight of the companies they serve. Audit committees must monitor the activities of both the internal audit and registered public accounting firm conducting the annual financial audit as well as the internal controls over the financial reporting process. Adequate compliance with the Act requires an active and open communication process between specific employees and the audit committee.
7. *Have you recently evaluated the risks facing your business?* Does your business have a process for evaluating business risk, regulatory risk, environmental risk, and internal process risk? Is risk considered in the planning of internal audit work and the registered public accounting firm's annual financial audit? Are business, financial, operating, and strategy plans developed with a risk assessment and mitigation plan? Are internal control processes designed to address the appropriate business risk factors challenging the company?

Risk is a significant factor affecting the performance of a company and its ability to comply with the Act. If risk can be effectively identified and understood, internal control processes can be designed and implemented to prevent, detect, and mitigate the identified risk and thus assist in assuring compliance with the Act.

8. *Do you receive complete and timely financial information necessary to make informed management decisions?* This question directly addresses the core requirements of the Act. If complete, accurate, and timely information is not readily available to all

Initial Compliance

levels of management, companies are not in a position to comply with the Act. Speed and accuracy are explicitly required to fulfill the mandates of Section 409 of the Act. Any weaknesses in financial systems should be adequately addressed and resolved in order to achieve compliance.

9. *Do you have key performance indicators that highlight issues that require attention?* A system of key performance measures, whether based on the Balanced Scorecard method, internal or external benchmarking, or some other performance measuring system, can serve as an early warning system if used properly. Such a system can be used to detect issues and monitor internal control and operating processes.

These questions can be helpful to compliance project leaders in assessing the current state of internal control, risk, and compliance. Subsequently, an effective compliance approach can be designed, developed, and implemented. Before implementing a compliance program, however, financial managers should address five additional key issues.

First, the impact to nonfinancial functions must be considered. How far beyond financial systems and controls do companies need to go? The answer to this question should be defined by the results of a comprehensive self-risk assessment process similar to the one addressed in Question 7. Internal control documentation must include all aspects of a transaction, including initiating, authorizing, recording, processing, and reporting. Information systems are probably the most significant of the nonfinancial systems with a potential impact on financial reporting controls. Other noteworthy areas to consider are risk management and human resources.

Second, the timing of remediation efforts may be critical. Companies should consider to what extent remediation efforts can be conducted in parallel with initial compliance activity. It is highly feasible, and a best practice, to plan for parallel documentation, control gap identification, gap remediation, and testing. Parallel execution can have a dramatic positive impact on both the cost and the time line of the compliance effort; however, it may also present several challenges. Considerations should be given to the following:

- Planning, preparation, and design should be integrated within the documentation phase before control gap remediation and testing begin.

Determining Organizational Readiness

- The compliance implementation team should have strong cross-functional representation and be staffed with experienced people (internal and/or external) who can quickly identify key control gaps and define effective remediation and testing criteria during the documentation phase of the project.
- To ensure the objectivity of the testing process, the process owner should not conduct final test design and implementation activities.
- Projects that have a high degree of parallel activity typically require full-time and experienced project leadership.
- All Act compliance efforts, especially those with a high degree of parallel activity, should be completed in collaboration with external auditors and have specific key checkpoints to ensure that the external auditors agree with the program direction and deliverables.

Third, companies must consider whether or not new software applications are necessary to effectively and efficiently complete compliance efforts. This is one of the most common dilemmas facing compliance project leaders. Since compliance is generally not predicated on the use of any specific software application, an effective approach may be to simply continue to use the tools already available, invest only as required for specific needs, and then select a new tool that will support ongoing compliance efforts. The market for Sarbanes-Oxley-specific compliance tools is slowly emerging and has significant potential for long-term benefits, especially in the management and execution of an ongoing compliance program. Companies should resist the urge to heavily invest in a compliance application that will not meet their overall long-term objectives. Patience in this area may reap significant long-term benefits. Potential system investments include areas such as document repositories, continuous control monitoring, internal audit management, risk assessment, self-assessment surveys, and performance monitoring systems.

Fourth, leadership of the compliance program must be formally identified. This decision is solely dependent on the unique needs of a company; however, this is a critical responsibility and should not be considered a “collateral” duty or one that is delegated to middle management. To ensure success, this responsibility must have executive level sponsorship or ownership, a high degree of interaction with the entire executive team and the board of directors, as well as sufficient resources dedicated to the project. Many companies will choose to designate a dedicated compliance officer, but all companies should involve senior management in the compliance effort.

Initial Compliance

Finally, resource requirements must be determined. For initial compliance, resource requirements can be effectively divided into two categories: project management and implementation resources. Every comprehensive compliance effort will require highly qualified experts in Sarbanes-Oxley Act requirements, SEC implementation rules, and PCAOB auditing standards and other pronouncements. If this expertise does not exist internally, companies should consider hiring full-time employees with the requisite experience and knowledge or consider engaging a qualified, independent consulting firm to partner with the executive management team to ensure successful Act compliance planning and implementation. Many companies will successfully manage the compliance effort with a mix of internal and external resources, and may engage more than one external consulting firm to handle different aspects of compliance. Companies with strong planning and project management resources may want to consider an external staffing firm to provide subject matter expertise and/or additional resources necessary to successfully implement the plan.

COMPLIANCE IMPLEMENTATION CHALLENGES

Regardless of the compliance approach chosen to manage the compliance effort, companies should consider the “spirit” of the Act, as opposed to just the letter of the law. The spirit of the Act inspires organizations to examine their corporate values and cultures; implement policies and guiding principles across the organization, not just accounting polices; manage information with effective internal control; hold the entire organization to a high level of accountability; and drive continuous improvement throughout the enterprise (see Exhibit 3.2).

Incorporating the spirit of the Act into the compliance delivery framework allows a company to go beyond mere compliance to promote cultural change within the organization by encouraging employees to view Act compliance and corporate governance not as an event, but as a way of doing business. Bringing about cultural change is just one of many key challenges financial managers and compliance project leaders will face in implementing a compliance framework. Other key challenges include:

- *The degree and character of executive support.* Without strong executive support, Act compliance will become a tenuous activity. In addition, the implementation is more likely to fail, experience cost

Determining Organizational Readiness

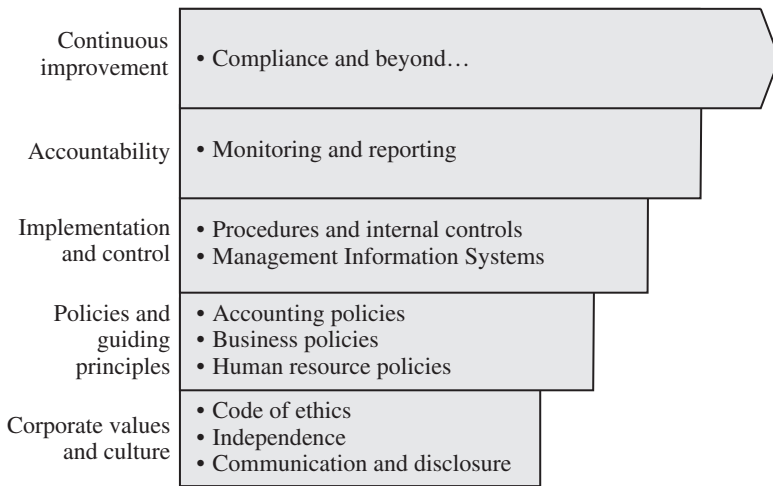


Exhibit 3.2 Sarbanes-Oxley Compliance Concepts: The Spirit of the Act

and time overruns, and foster key employee turnover. If executive commitment is a problem within an organization, engaging external consultants who specialize in Sarbanes-Oxley compliance activities may help to change the degree and character of executive support for compliance implementation activities.

- *The degree and character of operational acceptance and participation.* Operational, or employee, acceptance and participation often stems from executive support. If executives do not fully embrace and drive the compliance efforts, neither will the majority of employees. Unless a vocal majority of employees drive the process, bottom-up led initiatives are generally doomed to failure.
- *Depth of activity.* The greater the scope of the effort, the greater the time commitment and expense. However, scaling down the effort too much could lead to internal control failure and potential compliance failure.
- *Efficiency and cost/benefit analysis.* An effective cost/benefit analysis process is critical to effectively analyzing and determining the depth and breadth of the compliance efforts. Part of that analysis should include evaluation of the efficiency and effectiveness of existing internal controls.

Initial Compliance

- *Capturing value in the compliance initiative.* Compliance activity can become a springboard for productivity improvements, greater efficiencies, and competitive advantages in the marketplace.

When compliance is viewed as an opportunity to increase organizational performance and minimize risks, stakeholders are more likely to embrace the initiative and better results may be obtained. Chapter 4 outlines a preferred compliance implementation approach, the path to demonstrate compliance (“the Path”).

NOTES

1. PricewaterhouseCoopers Results of Survey of Sarbanes-Oxley Section 404 Project Leaders at Major Corporations, January 2004.
2. FEI Survey on Sarbanes-Oxley Section 404 Implementation, January 2004. Available on the FEI web site at www.fei.org.
3. *Id.*
4. *Id.*
5. *Id.*
6. *Id.*
7. *Id.*
8. *Id.*
9. Parson Consulting Survey report. Implementation Challenges of Sarbanes-Oxley Section 404, March 2004.
10. *Id.*
11. *Id.*

THE “PATH” TO COMPLIANCE

The Path to Compliance (“the Path”), is a six-step compliance framework that integrates the Committee of Sponsoring Organizations (COSO) framework of control objectives and control components (see Exhibit 1.2). Each step along the Path (see Exhibit 4.1) includes critical actions necessary to help ensure Act compliance and critical checkpoints to keep compliance efforts focused and on schedule. As with any compliance approach, the Path will require modification to the specific needs and circumstances of an individual organization and will become a reflection of available resources, committed time, and the qualifications of the employees dedicated to the compliance effort.

Step 1. Plan

- Establish project steering committee
- Form project team and establish project charter
- Develop actual compliance program planning
- Checkpoint: external auditor considerations

Step 2. Review

- Control reviews and assessments
- Documentation
- Gap analysis
- Checkpoint: documentation standardization

Exhibit 4.1 The Path to Demonstrate Compliance

Initial Compliance

Step 3. Improve

- Establish and/or change
- Checkpoint: identify streamlining opportunities
- Close gaps and strengthen internal controls
- Checkpoint: continuous control evaluations

Step 4. Test

- Train finance and operations staff
- Assign responsibilities for compliance
- Conduct internal testing
- Checkpoint: registered public accounting firm attestation engagement
- Prepare evidential documentation

Step 5. Certify

- Audit testing
- Checkpoint: draft certification disclosures
- Management certifications
- Auditor attestation

Step 6. Monitor

- Implement continuous monitoring process/system
- Checkpoint: internal control status reports to audit committee
- Ongoing compliance for Sections 302 and 404
- Demonstrated compliance!

Exhibit 4.1 (Continued)

PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD AUDITING STANDARD NO. 2

Before addressing the specifics of the Path approach, it is first necessary to understand the meaning of the key terms used during a review of internal control over financial reporting. While compliance with the Act is limited to such a review, the Path approach is also easily applied to internal control over operations. Public Company Accounting Oversight Board (PCAOB)

The “Path” To Compliance

Auditing Standard No. 2 (AS2) establishes the requirements and provides direction to external auditors in conjunction with an audit of internal control over financial statements. Since this is the standard by which the external auditor will conduct the review and attestation of internal control over financial statements, it also should be the basis for company self-assessment and should be integrated into the overall approach. All members of the project team must be thoroughly versed in the provisions of AS2, including the definition of internal control over financial reporting, control deficiency, significant deficiency, and material weakness, as well as the concepts of materiality, significant account, relevant assertions, and significant process.

Internal Control over Financial Reporting

PCAOB AS2 defines internal control over financial reporting as a company’s process, including policies and procedures that reasonably assure the reliability of financial reporting as well as the integrity of financial statement preparation process. The exact definition is contained in Appendix E. The definition places the responsibility for this process with senior management, including the board of directors. It specifically requires adherence to generally accepted accounting principles (GAAP) and inherently requires compliance with applicable laws and regulations affecting financial statement preparation and reporting.

AS2 further requires companies to maintain internal control over financial reporting policies and procedures that:

- Pertain to the maintenance of records that, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the company.¹

Companies must maintain transaction records that enable the company to support, and external auditors to substantiate, the accuracy of information contained in the financial statements. The main purposes of the maintenance of financial records are to ensure 1) the preservation of sufficient detail and documentation; 2) the existence of backup data; 3) a formal disaster recovery process; and 4) a formal record retention process.

- Provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with GAAP, and that receipts and expenditures of the company are

Initial Compliance

being made only in accordance with authorizations of management and directors of the company.²

All transactions must be recorded properly to facilitate accurate preparation of financial statements. An organization should maintain appropriate delegation of authority schedules that document the authority of employees to conduct transactions for the company as authorized by the board of directors and management.

- Provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use, or disposition of the company's assets that could have a material effect on the financial statements.³

In other words, the internal control over financial reporting must include specific controls to reasonably prevent and detect fraud in order to prevent material effects to the financial statements. The key phrases in this definition are “reasonable assurance” and “material effect.” There is virtually no way for companies today to prevent all instances of fraud, so they must implement controls that prevent and detect material fraud and make fraud difficult to commit. For example, segregation of duties is a reasonable control for the prevention of fraud in most processes; however, it cannot prevent collusion. The control typically works because it is unlikely that companies will have multiple corrupt employees working within a given process.

Control Deficiency

AS2 defines a control deficiency as a condition existing “when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis.”⁴ AS2 classifies control deficiencies as either deficiencies in design or deficiencies in operation. A design deficiency exists when a necessary control is missing from the process or the control function is improperly designed. An operation deficiency occurs when an employee fails to perform the control properly or when a properly designed control fails to operate as designed.

Significant Deficiency

AS2 states that a “significant deficiency is a control deficiency, or combination of control deficiencies, that adversely affects the company's ability

The “Path” To Compliance

to initiate, authorize, record, process, or report external financial data reliably in accordance with generally accepted accounting principles such that there is more than a remote likelihood that a misstatement of the company’s annual or interim financial statements that is more than inconsequential will not be prevented or detected.”⁵ The two key concepts here are “remote likelihood” and “more than inconsequential.”

For the definition of “remote likelihood,” AS2 simply incorporates the definition of “remote” as prescribed in paragraph 3 of Financial Accounting Standards Board Statement No. 5, *Accounting for Contingencies*:

When a loss contingency exists, the likelihood that the future event or events will confirm the loss or impairment of an asset or the incurrence of a liability can range from probable to remote.⁶

This statement uses the terms *probable*, *reasonably possible*, and *remote* to identify three areas within that range:

- *Probable*. The future event or events are likely to occur.
- *Reasonably possible*. The chance of the future event or events occurring is more than remote but less than likely.
- *Remote*. The chance of the future event or events occurring is slight.

Thus, for the probability of a misstatement to be more than a remote likelihood, its occurrence must be either probable or reasonably possible.

The clarification of “inconsequential” in AS2 is based on the “reasonable person” concept. If a reasonable person would conclude that a misstatement is immaterial to the financial statement, then the misstatement is inconsequential. On the other hand, if a reasonable person cannot come to that conclusion, by definition a misstatement must be deemed more than inconsequential.

Material Weakness

AS2 defines a material weakness as “a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the annual or interim financial statements will not be prevented or detected.”⁷

Whether a control deficiency exists and how to classify the deficiency will require judgment of the person performing the review or the external

Initial Compliance

auditor and should be based on the provisions of paragraphs 130 through 137 of AS2 (see Appendix F). A pictorial display of the hierarchy of internal control failures as contained in Exhibit 4.2 will assist in the classification of control deficiencies.

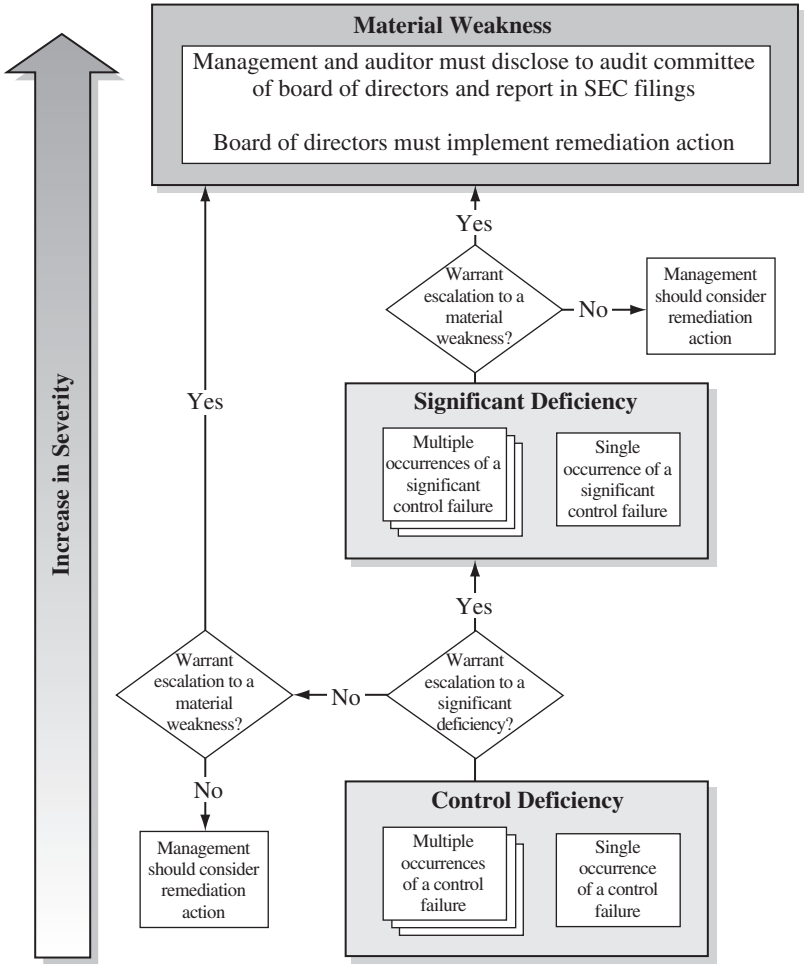


Exhibit 4.2 Internal Control Failure Hierarchy

The “Path” To Compliance

Materiality

Materiality is a concept that should be familiar to all financial managers and members of their project teams. It is a term used to describe the significance of specific financial statement information. The Financial Accounting Standards Board (FASB) Statement of Financial Accounting Concepts No. 2 defines materiality as “the omission or misstatement of an item in a financial report is material if, in the light of surrounding circumstances, the magnitude of the item is such that it is probable that the judgment of a reasonable person relying upon the report would have been changed or influenced by the inclusion or correction of the item.”⁸ AS2 specifically states that external auditors should apply the concept of materiality in the evaluation of the internal controls over financial reporting. The classification of control deficiencies as either a significant deficiency or material weakness is dependent on the concept of materiality. Materiality for internal control over financial reporting purposes includes both qualitative and quantitative factors.

Significant Account

Significant accounts as described in AS2 are those accounts that could have a material effect on the financial statements if such accounts contained one or more misstatements. The risk of misstatement in determining whether an account is significant includes overstatements, understatements, and omissions and should include both quantitative and qualitative factors. In reality, all accounts could be classified as significant under specific circumstances. The key determining factors are professional judgment and the application of the concept of materiality. It is critical that project plan classification of significant accounts be coordinated with the external auditor.

Relevant Assertions

Financial statements routinely include management assertions. In reviewing significant accounts, management assertions should be considered for relevancy. Statement on Accounting Standard (SAS) No. 31 classifies management assertions in the following five categories:

Initial Compliance

1. Existence or occurrence
2. Completeness
3. Valuation or allocation
4. Rights and obligations
5. Presentation and disclosure

Because relevant assertions have a direct affect on the accuracy of financial statements, the project plan listing of significant accounts should include references to the specific management assertions that are relevant to each account in order to determine the integrity of the financial reporting process.

Significant Process

The determination of significant accounts is the basis for identifying significant processes, because the processes are the basis by which accounting transactions are recorded to specific accounts. Included in this process is the determination, via review of account activity, of major classes of transactions for each significant account. Major classes of transactions include routine, nonroutine, and estimation and are defined as follows:

- Routine transactions are recurring financial activities reflected in the accounting records in the normal course of business (e.g., sales, purchases, cash receipts, cash disbursements, and payroll).
- Nonroutine transactions are activities that occur only periodically (e.g., physical inventory, depreciation expense calculation, and adjusting for foreign currencies). A distinguishing feature of nonroutine transactions is that data involved are generally not part of the routine flow of transactions.
- Estimation transactions are those that involve management judgment or assumption in formulating account balances in the absence of a precise means of measurement (e.g., determining the allowance for doubtful accounts, establishing warranty reserves, and assessing assets for impairment).

After identifying the significant accounts and the related classes of transactions, it is a simple step to determine the processes that control the

The “Path” To Compliance

transactions affecting the significant accounts. These are the significant processes that should be included in the compliance project plan. Typical in-scope major processes include order to cash, procure to pay, financial reporting and general ledger, inventory management, hire to retire, treasury and capital markets, asset management, capital planning, tax, equity, and information technology.

THE PATH TO COMPLIANCE STEP 1: PLAN

This is a critical stage in any project management effort. If priorities are not established from the start and effectively organized and mapped, the project team may be constantly distracted instead of driving toward a successful implementation. Companies must resist the urge to immediately delve directly into compliance activities such as documentation, testing, identification, and remediation of control deficiencies. While the planning stage may seem tedious, it is the cornerstone of effective project management. Extra care and consideration to thoughtful planning early on will provide project team members with a clear and precise understanding of their objectives and will help ensure that Act compliance objectives are met on time and within budget. The Path plan must be developed to ensure that it allows sufficient time for management to be able to make certain assertions concerning its internal control over financial reporting and for the external auditor to review such assertions, as well as to test, attest, and report on management’s assessment.

Establish a Project Steering Committee

The first action necessary for effective compliance is the determination of who is in charge of the project. While many companies will appoint a compliance officer or project manager to lead compliance activities, overall responsibility should remain with the board of directors and executive management. In order to ensure oversight, a steering committee should be established with the designated compliance officer as a standing member and a working group to deal with specific process issues. The steering committee should consist of five to seven senior executives including the chief financial officer (CFO) and representation from finance, operations,

Initial Compliance

internal audit, and information technology. This constituency should help ensure the efficient and effective resolution of issues and concerns. Steering committee discussions should include policy and standard setting. The steering committee should be a vehicle for rapid decision making and facilitate, not hinder, compliance implementation.

Form a Project Team and Establish a Project Charter

Project team members must be identified and mentored under the guidance of the compliance officer and the steering committee. A project charter should be developed and approved and endorsed by the steering committee with full board awareness. The project leader is undoubtedly the person with most influence over the outcome of the compliance effort. This person should be uniquely knowledgeable and versed in the requirements of the Act (as well as Securities and Exchange Commission [SEC] rules and PCAOB standards and pronouncements) and should possess exceptional project management skills and experience. Lack of these skill sets in the project team can, at a minimum, cost companies countless delays and costly overruns. Companies without employees with these capabilities should consider engaging an experienced external consulting firm to fill this role.

The project charter is analogous to company bylaws. It states why the project team exists and how it will operate to meet the goals of the project. The project charter is not a detailed plan of the steps required to achieve compliance.

The exact size of the project compliance team is not practically determinable at this point. While companies should estimate the resources necessary to implement the compliance plan, the actual resources necessary to complete the project will not be finalized until the detailed project plan is developed. Project scope change is often inevitable, and changes to the project plan will be necessary as actual process documentation and testing commence.

Conduct Actual Compliance Program Planning

During this stage, the scope of compliance efforts should begin to become clearer and measurable. In order to jump-start the planning process, many

The “Path” To Compliance

companies may benefit from conducting facilitated workshop sessions with the project team. The expected outcome of a facilitated session is:

- The identification of specific strategic and tactical decisions for the compliance initiative
- Development of a list of questions requiring resolution
- Identification of the necessary actions needed to advance the compliance initiative
- Specification of documentation form and content
- Confirmation of the work effort for the compliance initiative, including time and resources (both internal and external)
- Commencement of the creation of a detailed project plan

With these data as a foundation, the project team should determine and finalize the approach (including documentation templates), scope, and timing of the compliance activities as well as a methodology for resolution of any identified control deficiencies. The scope of the project includes the determination of significant accounts, major classes of transactions, and management assertions. This should enable the project team to identify the significant processes to be documented. A specific work plan with well-defined project team roles and responsibilities should be developed. The plan should also include the specific tasks to be completed as well as their sequence, the expected duration of the tasks, task assignments, expected outcomes of the tasks listed, and critical project milestones. Other key aspects of the project planning process include:

- Development of project activity time lines
- Final determination of project resources
- Inventory of processes by location
- Inventory of existing process documentation
- Training plan for project team members as well as finance and operations staff and resulting training materials
- Pilot process selection (used to test and confirm compliance approach)
- Process automation tool consideration
- Development of an effective communication plan

Initial Compliance

Checkpoint: External Auditor Considerations

After thorough analysis of the key compliance plan requirement components and the development of the detailed project plan, the initial compliance program should be communicated and approved by the steering committee. The project plan should then be reviewed by the external auditor to ensure that it incorporates internal control documentation requirements, expectations, and level of required effectiveness testing. The plan should be edited based on external auditor comments prior to moving into the implementation process.

Step 1 Expected Outcomes

The expected outcomes of Step 1 are:

- Establishment of a steering committee, project leader, and project team
- Creation of a project charter
- Development of a significant process listing
- Development of an inventory of existing process documentation
- Creation of a training plan for both project team members and financial and operational staff members as appropriate
- Detailed project plan

STEP 2: REVIEW

Once the compliance project plan is complete, a control environment review and risk assessment can begin. This activity should be followed by the documentation of current processes and controls and subsequent review of the adequacy of internal controls. It is also important to review the compliance project plan for modifications after completing the control environment review and risk assessment. At this point, consideration should be given to implementing weekly status reports for distribution to the project team with an executive summary distribution to the steering committee, key executives, and applicable members of the audit committee.

Control Environment Review and Assessment

After the overall compliance program is planned, an initial risk assessment of the control environment should be conducted. The initial control self-assessment should include an entity level risk assessment, a business unit risk assessment, and a process level risk assessment. An entity risk assessment addresses risk residing at the overall organization level and applies to the entire company. A business unit risk assessment addresses risks residing at, and unique to specific business units within a company. A process level risk assessment addresses the risk at the business process or functional level such as inventory, procurement, and reporting.

The risk assessment of the control environment should also include analysis of information technology (IT) general controls documentation requirements, and outsourced functions. This risk assessment should be interactive and collaborative and should be conducted through interviews with members of the applicable management team as well as key process owners and participants. The use of a comprehensive questionnaire is an effective tool for ensuring that all relevant subject matter is addressed in the risk assessment process.

After completing a risk assessment of the control environment, the project team can assign priorities and finalize the project plan. A critical part of the final project plan is the selection of an appropriate pilot process cycle. The overall pilot process should include the documentation of a single process or subprocess. It should not be an overly complex process (i.e., documentation, assessment, testing, and review can be completed in less than three weeks). For example, accounts payable/cash disbursements is a major process cycle that consists of several subprocesses potentially including purchase requisition, receiving, invoice processing, cash disbursements, and expense reports. Depending on the complexity of the subprocesses, the pilot program may include a single subprocess such as cash disbursements, which is an easily understandable and manageable process for completion and review.

After the selection and completion of the pilot documentation, the final project plan and pilot results should be presented to the steering committee for approval. In order to complete the pilot program, a review of Steps 1 through 4 of this compliance approach should be conducted. The pilot process, as with the overall compliance project, should concentrate on the documentation of internal controls through a series of interviews as well as

Initial Compliance

through the observation of the accounting department and appropriate process owners and areas. The pilot results should be reviewed and discussed with the project team and the external auditors in order to secure confirmation that the materials created are consistent with the requirements and vision of the business and that the methodology should continue to be applied across the remaining business locations and processes. Adjustments to the methodology and process outputs should be identified and implemented as a result of this review and integrated into the finalized scope and detailed project plan.

Documentation

This step requires the review of existing internal control process documentation and the creation of additional documentation where required. Documentation is not only critical to understanding the control process, but is absolutely necessary to effectively evaluate, remediate, and test the internal control over financial reporting. There are several ways and different tools available for the documentation of significant processes and the underlying internal controls and procedures. The required level of detail of documentation should be reviewed and approved by the external auditor. To illustrate the documentation phase, a specific example of compliance documentation for a hypothetical company's accounts payable/cash disbursements process is presented in Appendix G. Appendix G sample documentation includes:

- Process flowcharts
- Supplemental narrative
- Control matrix
- Segregation of duties
- Process walkthrough
- Control test plan
- Corrective action log

The documentation process should include interviews with selected process owners. Collaborative business facilitation may be utilized to run effective process documentation workshops. After reviewing existing documentation and conducting employee interviews and process documenta-

The “Path” To Compliance

tion workshops, current and complete process documentation should be generated for each significant process identified in the project plan. All documentation should be finalized except for the execution of the control test plan and the corrective action log, which will be finalized after completing the actual process walkthroughs and identifying and correcting control gaps.

A control matrix that outlines the control components identified during the process documentation of each significant process (at this stage, consideration should be given to utilizing the Control Objectives for Information and Related Technology [COBIT] framework for information technology controls) should be created and reviewed. While Act compliance is limited to internal control over financial reporting, all three COSO control objectives should be considered, because the financial reporting process may be impacted by the effectiveness and efficiency of operations as well as compliance with laws and regulations. To ignore any of the COSO control objectives would be a control deficiency in the Act compliance process. “Accordingly, all controls that could materially affect financial reporting, including controls that focus primarily on the effectiveness and efficiency of operations or compliance with laws and regulations and also have a material effect on the reliability of financial reporting, are a part of internal control over financial reporting.”⁹

A control test plan for each significant process should be developed. The control test plan should include the following:

- Significant process tested
- Company, segment, division, department name, and location of the tested process
- RFC Control number for each control (cross reference to process flowchart and control matrix)
- Description of the control to be tested
- Type of control
- Supporting documents to be reviewed during testing
- Sample size
- Sample selection procedures

An example of a control test plan is included in the sample documentation package in Appendix G. The test plans should be reviewed with the

Initial Compliance

external auditor to ensure the extent of testing is adequate to provide at least the same level of assurance that the external auditor requires.

Checkpoint: Documentation Standardization

A critical checkpoint at this phase of the compliance project is verification that the documentation process is standardized throughout the organization. Lack of standardized documentation will not prevent the completion of the project plan nor will it prevent external auditor attestation of the process of internal control over financial reporting, but it may increase the time and cost associated with both. Inadequate documentation may be considered a control deficiency that could be considered in certain circumstance to be either a significant deficiency or a material control weakness.¹⁰ This risk can be mitigated by implementing standardized documentation requirements for the entire organization as part of the project plan and continuous verification of adherence to the standard.

Gap Analysis

The final Step 2 activities include the comparison of the identified controls for each documented process to the COSO and COBIT requirements; identification of control gaps; assessment of the potential impact of the gaps; definition of possible solution options; creation of a corrective action plan; and recording of the applicable information to the corrective action log. At this point, identified control gaps should be classified as control deficiencies. Since control testing does not occur until Step 4, the control deficiencies identified most likely fall into the category of design deficiencies and should be further classified as either a significant deficiency or material weakness. Control gaps resulting from control objectives that lack a corresponding process control should also be identified and listed.

Step 2 Expected Outcomes

The expected outcomes of Step 2 are:

- Finalized project plan
- Pilot documentation results

The “Path” To Compliance

- Presentation of project plan and pilot documentation to steering committee
- Steering committee approval of project plan
- Documentation of significant processes, including:
 - Process flowcharts
 - Supplemental process narratives
 - Control matrix
 - Process walkthrough
 - Control test plan
- Weekly status reports
- Gap analyses with solution options and action plans

STEP 3: IMPROVE CONTROL ENVIRONMENT

In Step 3, it may be necessary to establish or change processes, identify opportunities for process streamlining, strengthen internal controls, and train appropriate employees. This “improvement” step occurs after the significant control deficiencies have been identified and remediated.

Establish and Change Processes

Upon completion of the gap analysis in Step 2, potential process change options were identified. All of the control gaps and related correction options should be reviewed and analyzed collectively to determine if there is a pattern that would require a change in overall control strategy of the company. After developing the control strategy for the business, specific control objectives or tactics can be selected to “close” or correct the identified control gaps. By selecting the control tactic to correct control deficiencies in this manner, the business is reasonably assured that all corrective actions and resulting changes to significant processes are aligned with the overall needs, objectives, and strategies of the business.

The actions required to correct control deficiencies identified by the gap analysis from Step 2 may require changes more substantive than the implementation of simple control tactics. In some cases, control processes may require a significant redesign or the development of new processes,

Initial Compliance

and the project team should be given the authority to recommend major changes where it believes they are necessary. All of the required changes should be summarized by significant process for development of a remediation plan and subsequent approval.

Checkpoint: Process Efficiency Opportunities

While the objective of the Path is to demonstrate Act compliance, assessments of the effectiveness and efficiency of operations is recommended. Doing so will increase the scope, related time, and cost of the project, but the potential savings could at a minimum create a positive return on investment (ROI). Even if the assessment of the effectiveness and efficiency of operations is not specifically built into the project plan, such outcomes are a natural result of the compliance implementation process, especially those relating to financial processes. A review of the gap analysis specifically for business process improvements and streamlining opportunities should be conducted. Such opportunities have the potential to offset project costs and create a positive ROI.

Close Gaps and Strengthen Internal Controls

Once the potential business process improvement opportunities are identified, an overall control remediation plan can be designed and implemented. In actuality, the remediation plan will consist primarily of a series of corrective action logs. Corrective action logs are discussed in the documentation phase of Step 2, an example of which is included in Appendix G.

The corrective action log identifies the:

- Company, segment, division, department name, and location
- Process and process owner
- Control deficiency log or tracking number
- Description of the control deficiency, observation, or finding
- Source or documentation package identifying the control deficiency
- Date logged
- Corrective action required, including the development of new or revised policy and/or process documentation

The “Path” To Compliance

- Indication of whether it qualifies as a significant deficiency or material weakness
- Individuals responsible for the corrective action
- Planned date of completion
- Status
- Signature lines for key financial employee certification as to the accuracy of the log

The corrective action log should be summarized by significant process to create the overall remediation plan and include, by process, the total number of control deficiencies, significant deficiencies, and material weaknesses in addition to the individuals responsible for implementing the corrective action, planned date of completion, and the status of the corrective action. These data, along with an overall time line for required corrective action, form the remediation plan. This remediation plan including a prioritization should be presented to the steering committee and audit committee for their consideration and approval. Written communication of all identified significant deficiencies and material weaknesses to the steering committee and audit committee is strongly recommended.

Train Finance and Operations Staff and Assign Responsibilities for Compliance

Finance and operations employees will require training on new process policies and required internal control changes and/or additions before implementing the remediation plan. A training plan should be developed to ensure appropriate training for all affected staff.

Step 3 Expected Outcomes

The expected outcomes of Step 3 are:

- Development of control strategies and control tactics
- Process improvement/efficiency opportunities
- Corrective action logs for each significant process
- Prioritized remediation plan

Initial Compliance

- Written communication of all identified significant deficiencies and material weaknesses to the steering committee and audit committee
- Steering committee and audit committee presentation of remediation plan
- Steering committee and audit committee review and approval of remediation plan
- Detailed training plan for affected employees

STEP 4: TEST

While the gap analysis performed during Step 2 identified control deficiencies, the ultimate determination of the effectiveness of internal control over financial reporting cannot occur until the controls over significant processes are appropriately tested. Step 4 includes the execution of the control test plans for each identified key/primary control, and the preparation of this evidential matter for review by the external auditor.

Control Testing Plan

Project team members conducting the control testing should possess professional skepticism, knowledge of the control testing provisions of AS2, including the examples of significant deficiencies and material weaknesses described in Appendix F (see also Appendix H), and the American Institute of Certified Public Accountants Auditing Standards Board's Statement on Auditing Standards No. 95, *Generally Accepted Auditing Standards*, as in existence on April 16, 2003 (the PCAOB adopted this auditing standard on an interim basis in PCAOB Rule 3200T, effective April 25, 2003). The objective of the control test plan is to provide an appropriate basis for management to determine the design and operating effectiveness of the key internal controls identified during the documentation phase. Testing must be performed by project team members who are independent of the process or activity tested. The test results will form the basis of management's assessment of internal control over financial reporting included in annual reports. The external auditor will review the test results and conduct independent testing during the attestation process.

Appropriate testing procedures include inquiry, observation, inspection, performance of control activities, and examination of evidence

The “Path” To Compliance

necessary to support account balances. Testing also addresses the execution and effectiveness of key internal controls. Controls should be tested at both the entity level as well as the transaction or application level. The entire population of transactions over which a key control is performed forms the basis for selection of the test sample. This includes all significant locations and reporting units.

The following factors should be considered in deciding the extent of testing:

- The degree to which the control is relied upon as a basis for its assertion (the higher the degree of reliance, the more extensively the control should be tested)
- The relative importance of the potential errors that could result if the control is not functioning properly:
 - Materiality of the transaction
 - Complexity of the transaction
 - Volume of transactions
 - Frequency of transactions
- The competency of the person performing the control
 - Competence, integrity, and ethics of the employee performing the control
 - Employee’s independence from the related processing procedures
 - Degree and adequacy of supervision of the employee
 - Extent of employee turnover
- The effectiveness of internal controls at the entity level
 - Likelihood that a control can be bypassed
 - Potential for management overrides of the control
 - Potential risk of fraud
 - Extent of monitoring activities during the fiscal period
 - Likelihood that a control will operate as intended until year end
- Changes in related processes including the effectiveness of current controls after implementation of changes
- How often the control is performed
 - Automated controls testing—generally test the application for each programmed control for each type of transaction if supported by effective IT general controls

Initial Compliance

- Manual control testing is based on frequency of performance
 - Performed many times per day—test at least 25 items
 - Performed daily—test at least 20 items
 - Performed frequently, but less than daily—test 25% of the occurrences, but not less than 25 items
 - Performed weekly—test at least 5 items
 - Performed monthly—test at least 2 items
 - Performed quarterly—test at least 2 items
 - Performed annually—test at least 1 item

Management must consider that conclusions drawn on the basis of limited testing may differ from the conclusions drawn if all items under a particular control are tested.

Conduct Management Testing

In this phase of Step 4, the control test plans are executed and the results, observations, and exceptions are noted.

During testing, all exceptions must be analyzed based on the nature and cause of the exception, the type of financial misstatement that could potentially occur as a result of the exception, the materiality of the potential misstatement, and the ultimate classification of the exception as a control deficiency, significant deficiency, or material weakness. Once the exception is classified and investigated, it may be necessary to implement corrective measures to mitigate the risk, change the control, or change the process. Test results should be recorded on the transaction testing matrix, which is included in the sample documentation package in Appendix G. The transaction testing matrix is cross-referenced with the control test plan to assure all testing is accomplished and results are appropriately documented. Page 1 of the transaction testing matrix records the following:

- Significant process tested
- Company, segment, division, department name, and location of the tested process
- Numerical listing of each individual sample transaction test (transaction test number)

The “Path” To Compliance

- Description of the sampled transaction
- Date of the actual recording of the transaction
- Document reference for the transaction
- Listing of each specific control as numbered on the control testing plan and a yes or no indication of whether the control was effective for the tested transaction
- Written testing observations and comments

Page 2 of the transaction testing matrix, which is a summary of observed exception, records the following:

- Transaction test number (from page 1)
- Exception type
- Explanation of the exception
- Whether corrective action is required (yes or no)
- Proposed corrective action or the rationale for no corrective action
- Reference to the logging of the corrective action on the corrective action log
- Overall conclusion as to the operation of the controls over the specific significant process
 - Process controls are operating as management intends (yes or no)
 - Process controls are operating as management intends with only minimal exceptions that are explainable and require no corrective action (yes or no)
 - Further testing is required to determine if test results (numerous unexplainable exceptions) are an anomaly (yes or no, with a reference to the additional testing if yes)
 - Significant corrective action is required; documentation package will require modification to reflect implementation of corrective action, and process walk-throughs will be reperformed, as will process control testing (yes or no)
- Certification of the applicable financial officers

All corrective actions identified via control testing should be recorded on the same corrective action log that was initially generated in the “close

Initial Compliance

gaps and strengthen internal controls” phase of Step 3. This unified approach to identifying control deficiencies and tracking corrective action is a strong control for assuring all required corrective action is implemented. It also provides an audit trail for the external auditor’s examination.

Checkpoint: Attestation Engagement

Verify that the audit committee has finalized the engagement of the external auditor for the internal control over financial reporting attestation and that the related scope, timing, and cost is understood and communicated. If coordination with the external auditor has been ongoing throughout the compliance implementation, the attestation engagement is most likely finalized.

Prepare Evidential Documentation

In support of the impending external auditor attestation engagement, finalize the assembly of documentation for presentation to the external auditor. If the project team was diligent in completing recommended documentation during the process, this information should be readily available and sufficient to meet the external auditor’s needs. Actively engaging the external auditor throughout the entire process provides reasonable assurance that the internally generated documentation will meet the external auditor’s needs.

External Auditor Testing

During the external auditor testing process, the project team should be coordinating and facilitating the external auditor attestation review. The project team is the owner of all of the initial compliance documentation during the project. Having conducted the review, they are also in the best position to support the external auditor and coordinate the support efforts across the company. The project team is also best prepared to address any control deficiency questions/discussions that may arise from the attestation review. The quick resolution and retesting of identified control deficiencies is critical to completing the attestation process within the deadlines for filing the required annual reports. External auditor-identified control deficiencies should be controlled by the same process used for remediation and implementation of corrective action; however, the control deficiencies

The “Path” To Compliance

should be categorized, indicating that they arose from the external auditor’s attestation process. Any identified significant deficiencies or material weaknesses must be promptly communicated in writing to the audit committee and copied to the steering committee.

Step 4 Expected Outcomes

The expected outcomes from Step 4 are:

- Executed control test plans
- Completed transaction testing matrix
- Update corrective action log
- Written communication of all identified significant deficiencies and material weaknesses to the steering committee and audit committee
- Development of a revised remediation plan to include the corrective action necessitated by the control testing
- Steering committee and audit committee presentation of remediation plan
- Steering committee and audit committee review and approval of remediation plan
- Audit committee finalization of the engagement of the external auditor for the internal control over financial reporting attestation
- Preparation of evidential documentation in support of the external auditor attestation engagement
- Listing of external auditor identified control deficiencies (corrective action should be included in the corrective action log and the remediation plan)
- Written and timely communication of all external auditor identified significant deficiencies and material weaknesses to the audit committee

STEP 5: CERTIFY

Too many financial managers believe certification and attestation are the ultimate goals of Act compliance. While it is certainly a requirement and a stated goal, it is not the end of the process. Section 302 compliance

Initial Compliance

requires that all future quarterly and annual financial reports include a certification executed by the chief executive officer and the CFO, and Section 404 compliance mandates that annual reports include (1) an internal control report stating management's responsibility for internal control and management's assessment of internal controls for the most recent fiscal year, and (2) the external auditor's attestation to management's assessments. At the end of this step, all three of those documents will be complete; however, it is through the process of compliance planning, assessing, documenting, analyzing, testing, and remediation that compliance is truly achieved. Step 5 involves finalization of all documentation.

Checkpoint: Draft Certification Disclosures

To expedite the final reporting process, the steering committee should be utilizing the information generated by the project team to draft the required annual certification reports. Certification cannot be finalized until the remediation plans are implemented and any additional testing is completed. Preparation of the documents in anticipation of the results of any required retesting will facilitate the final report process. The draft reports should be provided to the audit committee for review and comment.

Management Certifications

Assuming the remediation plan and any required control activity retesting is complete, the draft certification disclosures and management's assessment of internal control over financial reporting can be finalized for inclusion in the annual report. The final certifications and assessment reports—along with a final report of findings from the project team indicating the status of internal control over financial reporting and the resolution of both the remediation plan and corrective action log—should be presented to the steering committee, audit committee, and certifying executives for final review, modification, and approval.

External Auditor Attestation

The organization should receive a copy of the external auditor's attestation. The external auditor should then communicate the results of the attes-

The “Path” To Compliance

tation directly to the audit committee, steering committee, and executive management.

Step 5 Expected Outcomes

The expected outcomes from Step 5 are:

- Draft management certification and internal control assessment
- Completion of the remediation plan and corrective action log
- Final management certification assessment reports presented to steering committee and audit committee
- Final report on Act compliance from the project team presented to steering committee and audit committee
- Approval of management certifications and assessment report
- Receipt of the external auditor attestation

STEP 6: MONITOR

The final step in the compliance process requires companies to implement an ongoing monitoring and maintenance plan. Sections 302, 404, and 409 each require compliance in future periods. Thus, Act compliance is not a one-time event, but an ongoing process.

There are basically two types of future state monitoring processes: continuous monitoring and testing. A continuous monitoring system is one that is built directly into the significant processes and control activities and occurs with a regular frequency. Specific testing systems are separate reviews that are conducted on particular processes and controls and often are the result of some triggering event. Both types of controls can easily be incorporated into a self-assessment program.

A lengthier discussion of ongoing maintenance and monitoring is included in Part 2.

If an organization diligently follows the Path approach from Step 1 through Step 6, it should be able to demonstrate compliance with the Act.

Initial Compliance

NOTES

1. Auditing Standard No. 2. An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements, Paragraph 7, effective pursuant to SEC Release no. 34-49884; File No. PCAOB-2004-03, June 17, 2004.
2. *Id.*
3. *Id.*
4. *Id.*, paragraph 8.
5. *Id.*, paragraph 9.
6. FASB, Statement No. 5, Accounting for Contingencies (FAS 5).
7. Auditing Standard No. 2. An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements, Paragraph 10, effective pursuant to SEC Release no. 34-49884; File No. PCAOB-2004-03, June 17, 2004.
8. FASB, Statement of Financial Accounting Concepts No. 2, Qualitative Characteristics of Accounting Information (Concept Statement No. 2), 1980.
9. Auditing Standard No. 2. An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements, Paragraph 15, effective pursuant to SEC Release no. 34-49884; File No. PCAOB-2004-03, June 17, 2004.
10. *Id.*, paragraph 45.

PART TWO

ONGOING MAINTENANCE AND MONITORING

CHANGE MANAGEMENT

Change is the one certain outcome of Sarbanes-Oxley compliance. Companies may change their practices, policies, or procedures. They may change their control structures, key controls, or operational processes. Some changes may be rapid and straightforward, while others may require the complete redesign of key processes. Change cannot be avoided, and it should be prepared for.

Companies going beyond compliance view their Sarbanes-Oxley efforts as more than just a project, but as a process to effect positive change throughout the organization. Act compliance is an opportunity to transform a culture into an environment where internal control and process improvement are recognized as key components of good business. Such a cultural shift cannot occur, however, if an organization is unable (or unwilling) to implement real-time change on a consistent basis.

Companies use many different methodologies to implement change, including balanced scorecard, process reengineering, and total quality management (TQM) (see Exhibit 5.1). The methodology chosen is dependent on culture, environment, and other business factors. The success of the change initiative is not necessarily driven by the methodology itself, but by the effective management of the process.

Historically, change has not been managed well at most companies. For example:

- 42% of all technology projects are abandoned before completion.
- 70% of all business process reengineering efforts fail to produce anticipated business results.
- 75% of companies experience a drop in productivity for up to one year after implementing an enterprise resource planning (ERP) system.
- Only 16% of software implementations are successful as planned.

Ongoing Maintenance and Monitoring

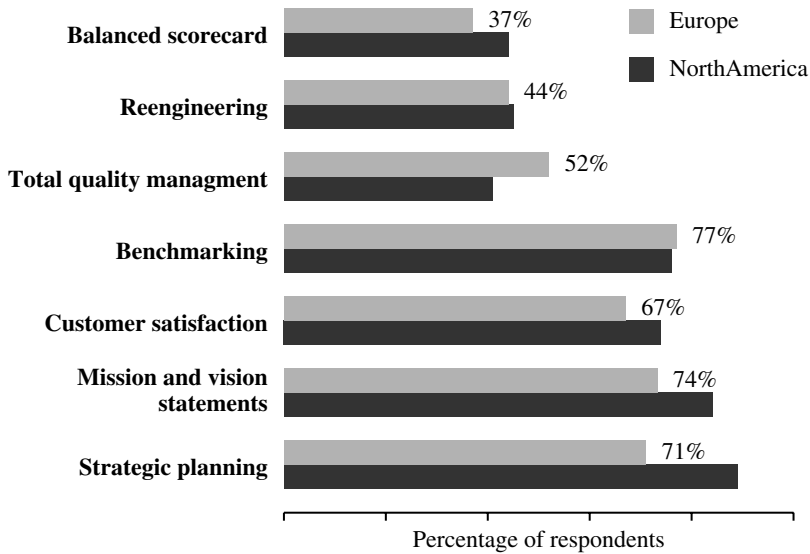


Exhibit 5.1 Change Management Methodologies and Techniques

Source: From a recent study of 475 companies by Bain & Co.

When change is not managed properly, the outcome is fairly predictable. Obviously, time and resources are wasted. Few things are more damaging to the work environment than having employees spend significant time and effort on a project that fails due to poor project management. In such cases, trust is often lost, which can lead to low employee morale and high turnover. Additionally, large sums of money are lost on redundant systems, ineffective employee training, and lower productivity. In the end, shareholder value may also decline.

Improving shareholder value is an intrinsic goal of all public companies and can be an outcome of Act compliance if a business embraces a culture of internal control and effectively plans, executes, and manages process change. In today's environment of increased governance, shareholders and analysts expect management to maintain at least adequate internal control systems. Anything less may result in a decreased perception of the company's worth and will negatively impact shareholder value.

READINESS FOR CHANGE

Successful change management initiatives occur when companies effectively begin the planning process by asking the question “Are we ready to change?” (see Exhibit 5.2). To evaluate the organization’s readiness for change, consider the following six questions:

1. *Is there a clear business reason for the change effort?* Companies often fail to ask this question or answer it honestly. Overlooking this question is probably the single greatest contributor to poor employee morale and a loss of trust. Employees will quickly conclude for themselves whether or not there is a compelling business reason for change.
2. *How well has the organization implemented other change efforts?* As with most initiatives, history is a good indicator of the future. Ask the same questions in the same way and you will get the same answers. Have past initiatives finished successfully or do they just end? Do they achieve the intended results? If there is a track record of failed initiatives, it is likely that future initiatives will fail too if the change management process is not evaluated and modified.
3. *Has executive management championed the project, and are they supporting it visibly?* This is critical to any change initiative, but especially so for Act compliance. You may have a problem with

- | |
|--|
| <ol style="list-style-type: none">1. Is there a clear business reason for the change effort?2. How well has the organization implemented other change efforts?3. Has executive management championed the project and are they supporting it visibly?4. How well does executive management understand the change process and its role in the process?5. Are business conditions appropriate to complete the project?6. Is the organization committed to providing resources (people, time, and money) to both design and implement change? |
|--|

Exhibit 5.2 Are You Ready to Change?

Ongoing Maintenance and Monitoring

management's commitment to the project if their response to compliance includes comments such as:

- a. "It's a necessary evil."
- b. "It's Congress's overreaction to a few isolated issues."
- c. "Let's just get it done for the lowest cost with the least amount of time and effort."

When it comes to compliance initiatives, the "tone at the top" is crucial to the success of the initiative. Management must visibly and actively embrace, participate in, and support the completion of the change initiative.

4. *How well does executive management understand the change process and its role in the process?* If executive management does not understand its role as champion of the change process, the project will begin at a disadvantage. Management must clearly communicate the need for change, the expected outcome, and how that outcome will benefit the company. Therefore, it is imperative that executive management clearly understand the process for change and how its role impacts the cultural environment, the success of the specific project, and the role of others.
5. *Are business conditions appropriate to complete the project?* It is extremely important that the business environment be conducive to change. If the business is stressed due to external factors such as a recession or slowing sales, change must be implemented carefully. Additional internal factors such as significant employee turnover, high levels of overtime, or poor operating performance could also lead to ineffective change initiatives. While many of these factors could be symptoms of the need for undertaking a specific action, such factors, if not clearly understood, could also hinder implementation.
6. *Is the organization committed to providing resources (people, time, and money) to both design and implementation of change?* This is a key dilemma for all companies considering change. There must be a balance between resource allocation and the bottom line. Most highly successful companies foster a culture that embraces change as a competitive advantage. If your company does not have a culture that endorses change, it must at least commit adequate resources to ensure success. This includes not just

Change Management

financial resources, but people and time as well. The organization must be confident that the level of resources is sufficient to complete the project as planned.

WHY CHANGE INITIATIVES FAIL

After addressing readiness for change, it is important to understand why change efforts fail or achieve less than planned results. The goal of all change efforts is to improve operations, gain greater efficiencies, or, in response to the Act, become compliant. Unfortunately, good intentions do not guarantee success.

So why do change efforts fail to meet planned expectations? There are many reasons, most of which are included in one of the following nine categories:

1. *Lack of a compelling, clearly articulated business reason for change.* The absence of a compelling reason for change makes it extremely difficult to rally people around the project. Nobody wants to be part of a project that has no clear purpose. It may also be difficult to obtain employee buy-in when a compelling reason for change exists, but the reason is not effectively communicated to the organization. In this case, an otherwise successful project could fail simply because employees lose motivation while working on a project that is perceived to add no value to the organization.
2. *No clear connection to the strategy of the organization.* Similar to the previous reason, this is a major contributing factor to employee motivation and morale. When undertaking a change initiative, one of the first questions should be, “Is the proposed change aligned with our business strategy, mission, and vision?” If it is not, why do it? All actions of a business should correlate with its strategic plan. When there is no clear alignment with the strategy, mission, and/or vision of the organization, employees may lack support for the change. For example, implementing a Materials Resource Planning (MRP) system for a manufacturing company may make good business sense, but it would not make sense if the business strategy was to outsource all manufacturing and assembly operations. In this oversimplified example, employees would question the need for an MRP system given the business strategy.

Ongoing Maintenance and Monitoring

The opposite problem of disconnected change initiatives and business strategies is lack of clearly stated mission and vision statements that dictate the direction of the company. This often leads to a “project du jour” syndrome where companies embrace every new process improvement, change initiative, or technology advancement idea that comes along. Lacking any clear direction, all new ideas are latched onto with a hope that it will be the change that turns the business around. Most of these projects will fail on their own accord, but sometimes an initiative that could have helped will fail because it was not completed before moving onto the next new concept.

3. *Piecemeal approaches to change initiatives.* Instead of planning the entire change initiative, companies will often take a piecemeal approach in an attempt to not overwhelm the business with a rapid transformation. This approach can prolong the project to the point where interest and motivation are lost. Other problems can occur when individual efforts are not well planned and the implementation becomes scattered or disorganized.
4. *Failure to include organizational redesign and process redesign when implementing technology solutions.* Companies often rush to implement new technologies and overlook whether their existing organizations and processes will effectively integrate with the new technology. As a result, companies usually take a fragmented approach to change, which can doom a project or at the very least lessen its benefits to the business (see Exhibit 5.3). Before undertaking any technology change initiative, consider the need to transform applicable processes and organizational structure as well as adequately prepare employees for the upcoming change.
5. *Lack of active, visible leadership.* Everyone knows what happens to a ship without a rudder—it cannot sail a straight course. When a visible leader does not actively lead change initiatives, they often end up with no clear direction. Project management is a key aspect of all change initiatives, and the leader must set clear objectives for the team. Employees need to know what is expected and when. Leaders of the initiative must set the direction and actively manage the process from start to finish.
6. *Lack of commitment from stakeholders, support organizations, and end users.* The greatest change initiative will fail if the

Change Management

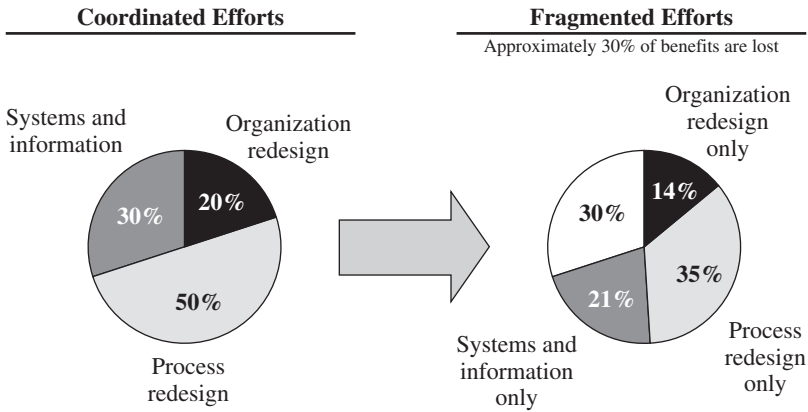


Exhibit 5.3 Fragmented Approaches to Change Initiatives

Source: Hackett Group

affected parties are not committed to the change. Since employees will ultimately have to use whatever system or process is being changed, early buy-in will certainly promote success. If you must rely on support organizations to complete a change initiative, make sure they are committed to the project and can provide resources to ensure a successful implementation.

7. *Undercommitment of time and resources.* A well-organized change initiative is only as good as the time and resources dedicated to it. Consider the need to backfill or hire temporary personnel to support the efforts of key employees. Getting the right balance of resources is key to success.
8. *Beginning communication, involvement, and training too late.* Keep all applicable employees involved and well informed from the start of the change initiative. If employees require training in order to work in the new environment, training should be conducted early enough so employees can effectively learn and practice, but not too far ahead of implementation that they forget what they learned before they have a chance to put it to practical use.
9. *Lack of skills and competencies to function in the future state environment.* Some companies get everything right, from tone at the top, to commitment of resources, to buy-in and communication, and their change efforts still fail for one simple reason—they

Ongoing Maintenance and Monitoring

failed to determine up front if their employees had the requisite skills to operate in the new environment. Some initiatives may require various levels of training to change the skill sets of impacted employees, but other changes may require a new set of skills for which training will not work. In such cases, existing employees may need to be transferred to other roles and new employees hired who possess the necessary skills. Consider the skill sets of employees early on to ensure success and prevent failure and/or costs from escalating.

KEY CRITERIA FOR CHANGE MANAGEMENT SUCCESS

On a macro level, successful companies use best practices to deal with cultural and organizational inhibitors to change. People and organizational factors are recognized as critical for business success and should be considered from the start of the planning process. Successful approaches to change management recognize that knowledge and understanding foster commitment, which leads to sustainability. And with sustainability comes long-term success.

People who see the implications of change on their daily lives tend to have a positive perception and are generally more committed to take the necessary actions to achieve the change. As a result, change management efforts of Sarbanes-Oxley initiatives that are in alignment with a company's business strategy will encourage process owners to *want* to do things the new way, which will ultimately lead to more successful results.

Successful companies also proactively transform processes while implementing new technology, but more importantly get buy-in from all necessary parties on process changes prior to the implementation. As stated earlier, 75% of companies experience a drop in productivity for up to one year after an ERP system implementation. The other 25% who did not lose productivity attribute this to:

- Successful user training
- A successful change management process
- Effective handling of risks and the fundamentals of project management
- Continued executive commitment

Change Management

For an overall change initiative to succeed, businesses must understand and focus on the key criteria for success (see Exhibit 5.4). First, all change initiatives must be clearly linked to the business strategy and communicated within the organization. The benefits of the change must also be easily understood, quantifiable (i.e., better, faster, less cost), and measured to properly track and measure success.

Furthermore, enterprise and interprise (the relationship between two or more business enterprises) implications must be analyzed and incorporated into the change initiative. An extension of that process is ensuring that key stakeholders, customers, and vendors are involved in the planning stage as well as engaged throughout the process. Involving all significant parties will allow an organization to build commitment to the project and help prevent surprises from materializing during later stages. The key is to maintain a high level of commitment and active involvement throughout the change effort.

- Change must be clearly linked to business strategy.
- Benefits must be quantified—better, faster, less cost.
- Enterprise and interprise implications are understood.
- Key stakeholders, customers, and vendors are engaged early.
- Organization, process, and technology issues are integrated into all change initiatives.
- Executive management champions the change.
- Leadership is clear, unequivocal, and consistent.
- Managers and employees are involved in the change process.
- Investments, including time and resources, are made to effect and sustain change.
- Education and training is built into change projects.
- Communication is ongoing, targeted, and personal.
- A communication plan unites all communication efforts.
- Both positive reinforcement and corrective feedback are used to facilitate change.

Exhibit 5.4 Key Criteria for Change Management Success

Ongoing Maintenance and Monitoring

All change initiatives should integrate organizational, process, and technology issues as much as possible. In businesses there is a natural nexus between these three components, and failure to take all three aspects into account often leads to a fragmented implementation. While they may be appropriate in certain situations, fragmented implementations typically contribute to change effort failure or a loss of benefit. Exhibit 5.3 shows that approximately 30% of the benefit associated with a change effort is lost when businesses apply a fragmented approach. The loss of benefit is not limited to any one of the three components, but is distributed across all three, with process redesign generally most affected.

Additionally, it is paramount that change initiatives be championed by executive management and that the champion stay actively or at least visibly involved in the entire process. The champion must select or oversee the selection of a project leader who is clearly endorsed by executive management and is given the appropriate level of authority to successfully complete the project. Project leadership must actively involve and motivate all employees associated with the initiative and must quickly react to any delays, implementation issues, or signs of declining employee productivity.

Project leadership is also responsible for estimating the proper level of investment in time and resources. Resource considerations must include appropriate levels of education and training, both for the implementation team as well as the users or process owners. Education must be properly designed and timed to accelerate learning. Much of the productivity losses associated with unsuccessful or delayed projects can be linked directly to the poor quality of instruction or an employee's inability to utilize changed systems or processes immediately following training.

Leadership must also develop and implement a communication strategy and plan, which focuses and unites all communication efforts internally and externally. Communication must be ongoing, targeted, and personal. It must also be credible and concise. The effect of communication, coupled with the tone from executive management and project leadership, will directly impact employee commitment to the project. Nowhere is this more important than with compliance initiatives such as those required by the Act. Executive management must honestly believe and effectively communicate the importance of maintaining a strong internal control environment not just for compliance, but also for good business and a competitive advantage. This approach will go a long way toward ensuring the success of Act-related change initiatives, particularly those addressing ongoing compliance.

INTEGRATED CHANGE MANAGEMENT

Understanding why change initiatives fail or succeed is instrumental to developing an effective approach to change management. This is not the same as management methodologies and techniques for change such as TQM and balance scorecard, but an approach to implementing one or more of such methodologies. The approach discussed here is called integrated change management (ICM) and has four key components (see Exhibit 5.5):

1. The uncontrollable external environment
2. The controllable external environment
3. The internal environment or integrated change components: organization, process, and technology
4. Business metrics and strategy

The ICM approach states that all four of these components intertwine and influence a company's ability to implement change, which moves the organization closer to the achievement of its mission. Take away any

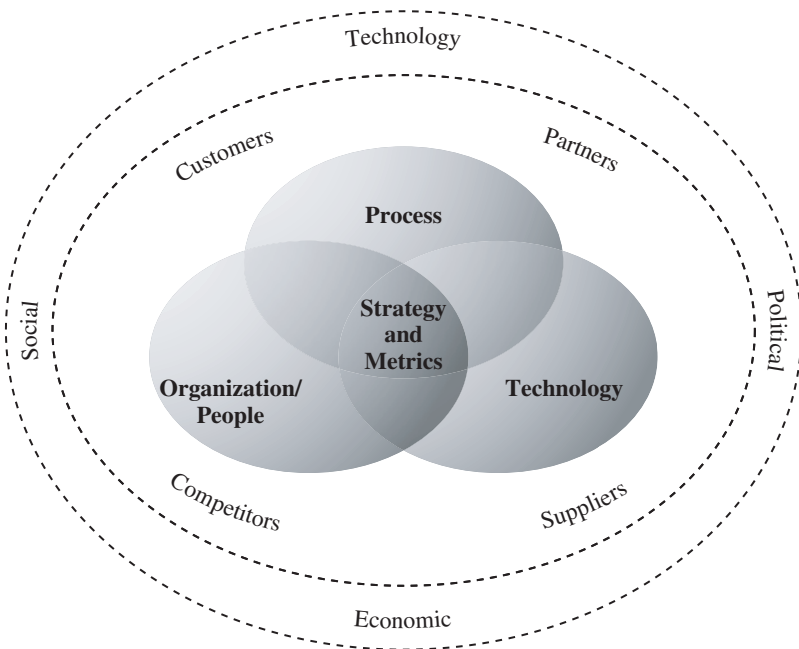


Exhibit 5.5 Integrated Change Management

Ongoing Maintenance and Monitoring

individual components and the critical drivers of a change initiative may be omitted, thus increasing the risk of project failure. Neglect to consider the social aspects affecting employees, customers, or competitors and you may miss competitive advantages available to you from a process change. Fail to consider the technology environments of partners, customers, and suppliers and you may implement a state-of-the-art system that is rendered useless because partners, customers, and suppliers have limited capabilities that prohibit them from effectively using the system.

ICM is best utilized when individual components are understood. The ICM approach displayed in Exhibit 5.5 may look a bit confusing, but it is actually quite simple to understand when applied from the middle outward, starting with business strategies and metrics. For purposes of ICM, it is assumed that the business strategy and key metrics are already aligned with the mission and vision of the organization. If this is not the case, this step must be accomplished before attempting any change initiative. Initiatives that are not aligned with a company's strategy, mission, and vision are predisposed to failure. If the change initiative to be undertaken is an overarching change such as implementing a unified control environment across all aspects of a business, the strategy and metrics must be viewed at the top level. On the other hand, if the change initiative deals with only one unique aspect or process of a business, such as the control environment over the petty cash process, the strategy and metrics must be considered on that level, but flow up to the top-level strategy. In any event, proposed changes should first be evaluated to determine whether they are in alignment with the overall strategy of the company.

Once it is determined that a proposed change will further the mission and vision, the key components of the internal environment must be considered—organization, process, and technology—to determine the initial plan for the change initiative. The review of the internal components should first evaluate the current state of the components and how they are related. For example, initial Act compliance activities may have disclosed control deficiencies in a particular process that require remediation. By the nature of the deficiency, the change effort will affect the specific process, but the company must also consider what impact the change may have on the organization and the employees. The same analysis must also be conducted for technology considerations. The interaction between any two components is most often two-way and will likely have a related effect on a third component. This interdependency is why the three internal environment components should be integrated into all change efforts. After

completing the review of the internal environmental components, an initial implementation plan should be developed that fully incorporates all of the key criteria for change management success included in Exhibit 5.5.

Next, the initial implementation plan should be refined to include controllable external environmental factors. This analysis simply asks two questions: “What impact will our proposed change have on our suppliers, partners, customers, and competitors?” and “How do our suppliers, partners, customers, and competitors impact our proposed change?” The answers to these questions are considered controllable external environmental factors because, while a company does not actually control these external organizations, its choices will, to varying degrees, affect them. They are also controllable factors in that a company can choose which organizations it uses as suppliers as well as from which industries it will attract customers and competitors. In this phase of the planning analysis, the company should also consider how the technology aspects of the change initiative impact suppliers, customers, and partners and whether their technology environments will facilitate or limit change initiatives.

The last step of the ICM approach is to consider the impact the uncontrollable external environmental factors may have on the revised implementation plan. These factors affect all businesses in some way, but may uniquely impact a business depending on the industry or organizational structure. While there are countless individual uncontrollable external environmental factors that may impact a change effort, the ICM approach groups them in four major categories: technological, social, economic, and political.

Political factors include the effects of local, state, country, or global governments on a business. These factors may be as simple as complying with foreign country accounting rules or as complex as dealing with international terrorism and political upheaval. Political factors are often unpredictable and subject to change at any time. They can also be contradictory, requiring compliance with differing political agendas at the same time. For example, all businesses from the United Kingdom with United States listings will have to comply with the provisions of the Sarbanes-Oxley Act. What makes this complicated is that they also have to comply with similar United Kingdom rules that necessitate two sets of compliance activities and reconciliation between the two.

The political environment typically drives the economic environment. Certainly in the United States the differences between the Democratic and Republican parties and their positions on issues such as taxes and government spending will have a significant impact on the economic environment. Other

Ongoing Maintenance and Monitoring

economic factors include interest rates, overall economic health (i.e., periods of inflation, deflation, growth, recession, or depression) and the condition of various industry sectors. Economic factors also include the overall health of the business industry. While rapidly increasing oil costs may arguably have a positive impact on gasoline refineries, it will have negative repercussions on the airline industry and tourism, which can have a ripple effect through other areas of the economy.

Social factors are generally based on the evolving moral standards of a culture. The Sarbanes-Oxley Act of 2002 was enacted partly in response to the social call for change in how businesses in the United States were being managed in light of several very public instances of corporate fraud. This societal impact has had a direct and large impact on how publicly traded companies are now managed. As a whole, social factors will vary based on the political environment and economic factors, but they ultimately develop from the moral standards of a society.

Technology, the final category of uncontrollable external environmental factors, must be considered at a macro level. Such factors are not limited to computer hardware and related peripherals such as software applications, communications equipment, manufacturing equipment, and processes. Technology encompasses all practical applications of knowledge to improve existing capabilities. Whatever technological changes are occurring in the world, their impact on the business and the particular change initiative must be assessed.

After all uncontrollable external environmental factors have been considered, the revised change plan, based on the ICM approach, should be transferred to an implementation framework. There are many different implementation frameworks that businesses can utilize; however, special consideration should be given to frameworks that include at least the following five steps.

1. Plan
2. Design
3. Build
4. Implement
5. Sustain

An example of a five-step implementation framework is presented in Exhibit 5.6.

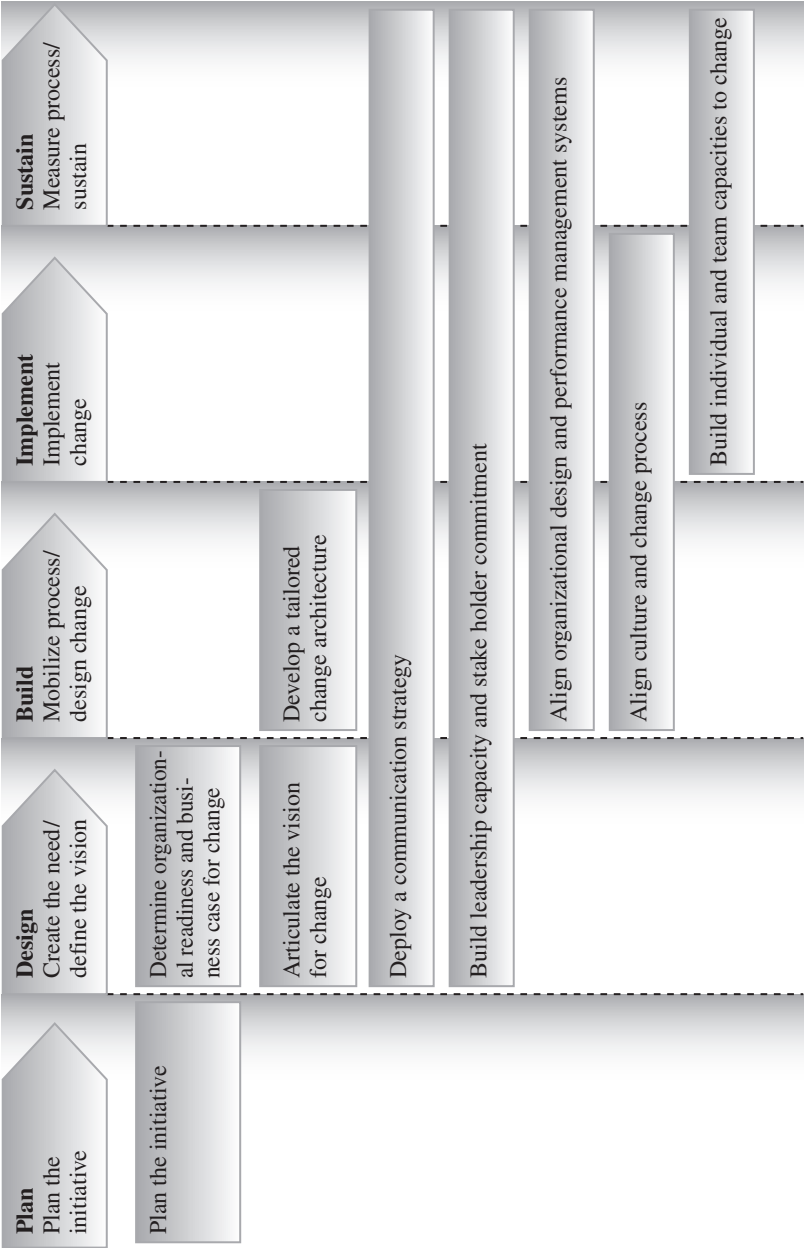


Exhibit 5.6 Change Management Implementation Framework

Plan

The Plan phase of the implementation framework is where the initial plan created as the outcome of the ICM approach effort is expanded to include details of the actual change initiative. The ICM plan determined what was going to change and how broad the change would be after considering the four key components: (a) business metrics and strategy; (b) internal environment or integrated change components—organization, process, and technology; (c) controllable external environment; and (d) uncontrollable external environment. In this stage, details of how the change initiative will occur are documented and mapped, and an initial time line for the implementation is developed with resources allocations, key milestones, due dates, and metrics. The plan should also include the roles of executive management, training needs, and the communication plan.

Design

The design phase addresses the need for change and refines and communicates a vision for the initiative. The organization's readiness for change is determined and any corrective action is swiftly implemented. During this phase, the change champion must motivate the organization, establish a position of authority, identify and secure the resources needed to successfully achieve the change, and foster stakeholder and employee commitment.

Build

The implementation plan is further refined during the design phase, but it is not until the build phase that the foundation for the implementation is firmly set. The communication strategy continues to be employed during this phase to keep all parties actively informed, which helps leadership to continue to build stakeholder commitment. The organizational readiness determination from the design phase is aligned with the change initiative to effectively address all cultural issues, and the implementation plan is integrated with the business's performance measuring system and key metrics.

Change Management

Implement

The actual implementation plan is now complete, and detailed time lines with deliverables and expected results are clearly outlined. Resources are committed, responsibilities are assigned, and the work begins. During this phase, leadership must use performance measurement systems and metrics to assess the success of the implementation.

Sustain

During this final phase, implementation results are measured against the detailed plan and time line in order to monitor progress. The communication strategy and leadership effectiveness are paramount in maintaining motivation. Throughout the five-step process, employees are trained as appropriate, but it is during the sustain phase that training is generally conducted so end users are prepared to utilize the new systems and processes immediately following implementation. The key to this phase is measuring results, making real-time modifications, and staying focused on the time line and desired results.

Most successful change initiatives result from a detailed plan that clearly communicates the need for change as well as the roles, responsibilities, and deliverables expected from *all* affected employees. Businesses that consistently implement successful change initiatives align their change efforts to their business strategies (mission and vision) and execute in the following six critical areas:

1. Leadership and management
2. Communication and selling
3. Measurement and accountability
4. Motivation and incentives
5. Skills and capabilities development
6. Organization and people

Exhibit 5.7 shows what will result if any one factor is missing from the equation. Lack of communication results in confusion. Lack of measurement results in false starts. Lack of motivation results in slow change.

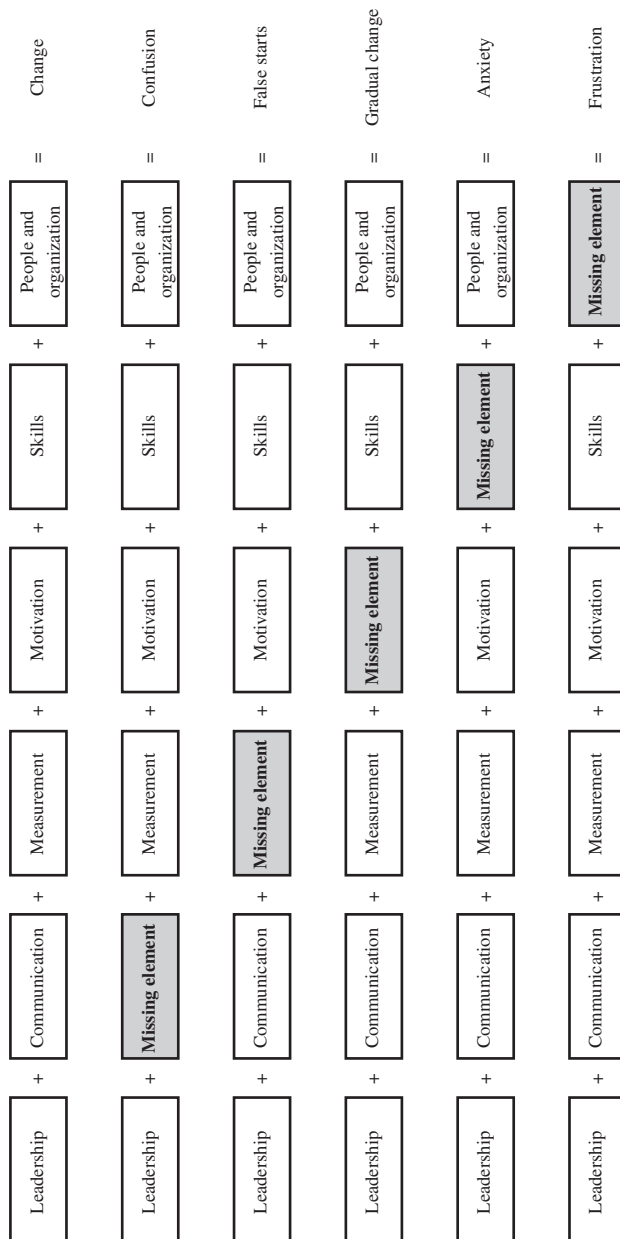


Exhibit 5.7 The Effects of Missing Change Elements

Change Management

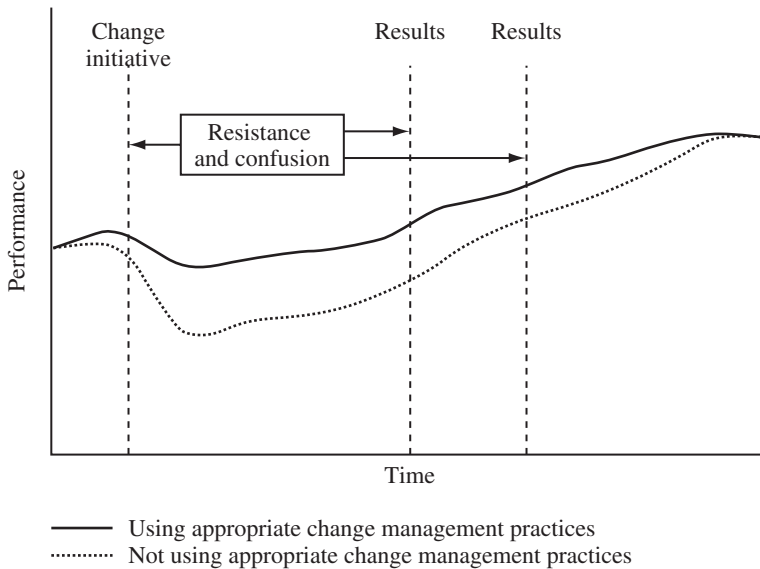


Exhibit 5.8 Results of Effective Change Management

Regardless of which component is overlooked, change efforts will be impacted.

A successful change effort is founded on a comprehensive approach such as ICM, utilizes an integrated implementation framework, and ensures there are no missing pieces to the change initiative. Effectively addressing these three critical aspects of change management will lead to better performance and faster results, as displayed in Exhibit 5.8.

ONGOING COMPLIANCE ACTIVITIES

Once an organization has achieved initial compliance, it should be reminded that compliance is not a one-time event. Testing, monitoring, and certification requirements recur on a quarterly and annual basis, requiring companies to sustain compliance until the Act itself is either abolished or amended.

To achieve sustainable compliance, companies should build an efficient and effective infrastructure that enables repeatable, reliable actions. In postimplementation years, compliance efforts will typically not be as great, but activities such as documentation, testing, and remediation will still need to be conducted throughout the year. Ongoing compliance will also require the linking of Section 404 monitoring efforts to quarterly reporting under Section 302, which requires quarterly evaluations and the reporting of any changes in internal controls over financial reporting that either have or could have a material effect on the financial statements. Accordingly, companies must develop the ability to keep their assessment of internal controls over financial reporting current throughout the year and cannot wait until the end of the fiscal year to evaluate changes in internal control.

Following initial compliance, it is important to effectively position the business to properly assess improvement opportunities and remediation requirements, elevate the role of the finance group, and evaluate the impact of the Act on operations. These elements are essential to a company's ability to sustain compliance.

IMPROVEMENT OPPORTUNITIES AND REMEDIATION EFFORTS

Current open remediation activities should be assessed before advancing to ongoing compliance activities. An integral component of both Step 3 and

Ongoing Maintenance and Monitoring

Step 5 along the Path to Compliance approach discussed in Chapter 5 is identifying, recording, and remediating identified control gaps. Ideally, a best practice is to complete remediation activities concurrent with compliance efforts.

The timing of compliance and remediation efforts is crucial to the certification of financial reports, the annual management assessment of internal control over financial reporting, and the related external auditor attestation engagement. Companies should consider to what extent remediation can be conducted in parallel with initial and ongoing compliance activity. It is highly feasible to plan for parallel documentation, control gap identification, and gap remediation. Such parallel execution can have a dramatic positive impact on both the cost and time line for compliance efforts.

Current as well as future remediation efforts should be designed to improve the efficiency and productivity of the impacted operating processes. Each internal control remediation gap should address how the corrective action not only improves the level of control, but also enhances the overall transaction process flow.

The first step in effectively coordinating various remediation requirements is to categorize them by type of improvement opportunity: internal control improvements, Sarbanes-Oxley and financial reporting improvements, or productivity improvements. Examples of each type of remediation category are as follows:

- Control improvements
 - Mitigate missing or deficient controls.
 - Eliminate unnecessary or redundant controls.
 - Minimize financial statement line items or process risks.
 - Eliminate policy and/or authorization deficiencies.
 - Establish control process breakage metrics.
- Sarbanes-Oxley and financial reporting improvements
 - Establish a Sarbanes-Oxley reporting package.
 - Establish data standards across financial processes, functions, and operations.
 - Minimize cost of ongoing compliance.
- Productivity improvements
 - Eliminate non-value added tasks.
 - Automate manual activities (e.g., reconciliations).

Ongoing Compliance Activities

- Establish data and/or process standards across regions.
- Revise policies.
- Align business activities and efforts with perceived value.
- Focus on revenue enhancement and cost reduction.

Improvement opportunities are then prioritized based on business impact and complexity (see Exhibit 6.1). Immediate priority improvements, or high-impact improvements, address material business issues and can be accomplished in a short duration with minimal business disruption. They mitigate significant business risk and typically yield results quickly. The implementation of high-impact improvements generally should not extend beyond 90 days. Secondary priority improvements are medium-impact initiatives that focus on material business issues; however, they

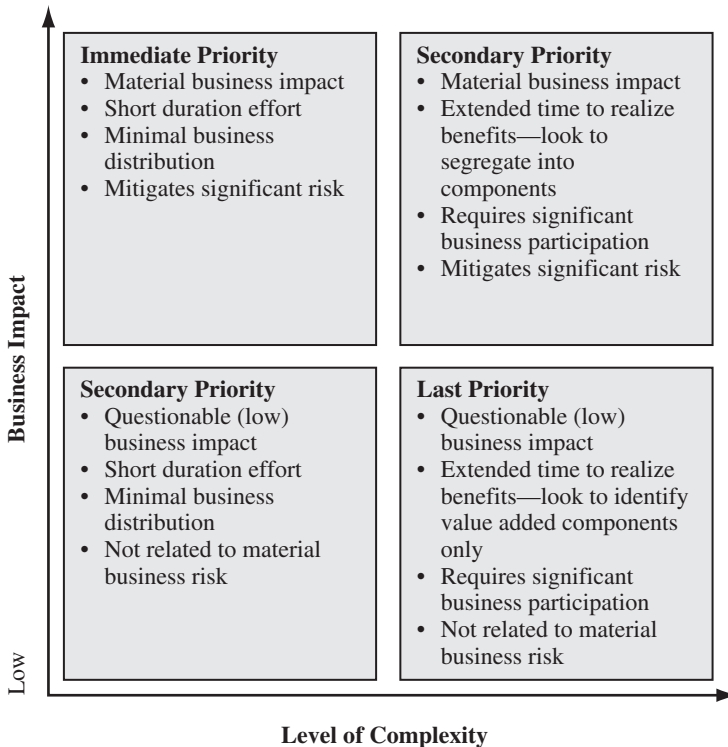


Exhibit 6.1 Improvement Opportunity Prioritization Matrix

Ongoing Maintenance and Monitoring

require an extended period of time and significant participation from the business to implement. The duration of medium-impact improvements will typically be between three and six months.

Prioritizing remediation activities based on process improvement opportunities will not only reduce the organization's risk in reporting and disclosures, but also elevate finance's position as a valued business partner.

THE ROLE OF FINANCE

Prior to Sarbanes-Oxley, chief financial officers (CFOs) and chief auditors often focused on "value added" activities like top-line initiatives, strategic acquisitions, and operational improvements. But the passage of the Act has moved internal controls, often previously regarded as secondary considerations, front and center. The goal now is to determine how finance can remain a valued partner to the business in an environment of increased governance.

Documentation efforts required by Section 404 have enabled many companies to launch the first step in business process improvements, namely documenting current processes and identifying redundancies and inefficiencies. As control remediation continues, companies are well positioned to incorporate current or future process improvements because the groundwork for understanding current processes (i.e., documentation) has already been performed. The four steps summarized below can help the finance department deliver continuous value to stakeholders in today's compliance environment. This process will be discussed in greater detail in Chapter 9, Process Improvement Considerations.

- Step 1. Identify the enterprise strategy and communicate it throughout the finance organization. Sarbanes-Oxley remediation and change initiatives should meet short-term goals and deliver long-term value.
- Step 2. Develop a finance strategy to support the enterprise strategy. Reevaluate existing key performance indicators and metrics to include crucial Sarbanes-Oxley processes.
- Step 3. Generate a capacity to provide analytical and consultative services. Remove non-value added processes that were identified during Section 404 documentation.

Ongoing Compliance Activities

- Step 4. Leverage technology to deliver and distribute results. Avoid manual workarounds and reduce the cost of ongoing compliance through technology.

Good governance, as evidenced by an effective system of internal control, and adding value to the business do not have to be conflicting objectives. Many businesses have recognized the compatibility of the two goals and have incorporated both perspectives into their planning and compliance programs.

OPERATIONAL STRUCTURES

An increased pressure to do things faster, better, and more cost effectively has prompted companies to pursue various strategies to improve operational effectiveness. What functions should be performed within the business units? Who should select, purchase, and operate the supporting technologies? When should business units be free to choose operating standards and when should corporate mandate consistency? These questions are answered differently based upon a company's operating style, industry, and market focus.

Since there are benefits to both centralization and decentralization, companies should closely examine both approaches before making any operational changes:

- Benefits of centralization/standardization
 - Less redundancy in operations
 - Leverage of management time and attention
 - Economies of scale
 - Easier implementation of best practice approaches
 - More defined career paths for professionals in support functions
 - Reduced maintenance costs and effort
 - More efficient utilization of information technology (IT) resources (e.g., technical infrastructure, application support and licensing, and modifications)
- Benefits of decentralization/customization

Ongoing Maintenance and Monitoring

- Processes and systems can be tailored to each business unit's unique needs
- Local systems can be more responsive to changes in business conditions
- Local operations can help foster a culture of ownership
- Local operations that are integrated through a monthly feed of summarized financial information to corporate can be more easily incorporated or divested

While there are benefits to decentralization, compliance requirements driven by Sarbanes-Oxley will likely make economies of scale more important. The expense and time required to annually review process documentation and retest will increase with each separate department engaged in auditable activity. This will be particularly true where operations are not only separate, but also vary in terms of systems, formats, and process design.

Centralization is not an easy change. Companies are often reluctant to move away from their decentralized structures (even if they know they are ineffective) because the social, technical, and financial costs of changing can be high. Nonetheless, more organizations are finding that the additional cost of complying with the Act warrants the decision to centralize or even employ a shared services model.

THE PATH TO ONGOING ACT COMPLIANCE

There are only subtle differences between initial compliance—as discussed in Chapter 4—and ongoing compliance. The major difference is that for many companies initial compliance with the provisions of Sarbanes-Oxley was achieved through a project-focused initiative. Even though the continuous nature of the Act requirements beyond the first year was understood, businesses took a project management approach to addressing Act requirements, which typically resulted in a large undertaking with a definitive beginning and ending point. Companies that took a best practice approach to initial Act compliance recognized the benefit to building ongoing processes into their initial compliance efforts, and focused on changing the culture of their businesses in order to embrace the need for stronger systems of internal control, change management, and process improvement. This course of action allowed them to lay the foundation for ongoing Act com-

Ongoing Compliance Activities

pliance as a process-driven initiative with the goal of continually meeting the requirements of Sections 302 and Section 404.

The cost associated with initial compliance was extensive. Most companies underestimated the total cost. Unfortunately, ongoing compliance costs are not anticipated to be significantly lower. Costs associated with ongoing compliance are estimated to be as much as 50% to 70% of the cost of initial compliance. The rationale for this estimate is understandable considering the work that still needs to be completed. The five major components of initial Act compliance—project/process management, documentation, testing, remediation, and reporting—are still required for ongoing Act compliance. Exhibit 6.2 portrays this point. All five components of compliance are present in both initial and ongoing compliance, with testing and reporting requiring the same level of effort. While this may seem counterintuitive, the reason is that Public Company Accounting Oversight Board (PCAOB) Auditing Standard No. 2 (AS2) requires management’s assessment of internal control over financial reporting to be as of a specific point in time¹ (i.e., the business’s fiscal year end). Prior fiscal

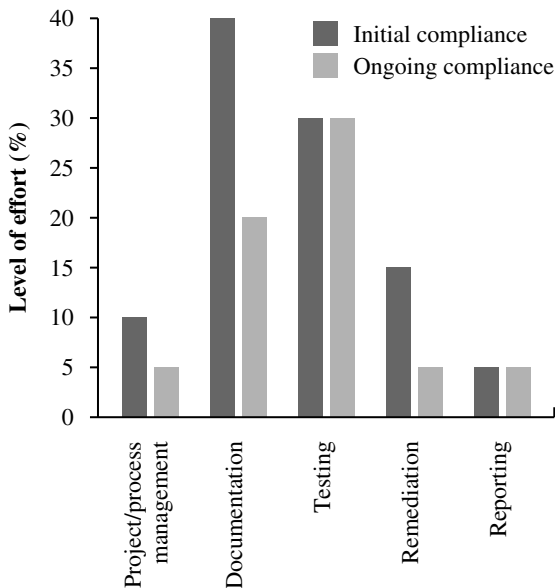


Exhibit 6.2 Compliance Effort Comparison: Initial Compliance versus Ongoing Compliance

Ongoing Maintenance and Monitoring

year testing cannot be utilized to satisfy the requirements of the current fiscal period management assessment. Slight changes in testing scope may occur from year to year based on the evolving interpretations of the extent of testing required to demonstrate the effectiveness of internal control.

The areas of significant cost savings in ongoing compliance are documentation and remediation. Ongoing documentation compliance efforts will be limited to only updating the documentation created during initial compliance and developing documentation for new systems or processes. A similar argument can be made for remediation efforts since most of the control gaps were identified and should have been closed during initial compliance. As the overall control environment strengthens, the frequency of future control gaps should decline, driving a resultant decline in required remediation efforts. Regardless of the level of effort required, maintaining ongoing compliance will be expensive, but can be partially offset by leveraging the documentation and information developed or gathered during initial compliance.

The Path to Ongoing Compliance (the Path) is a suggested approach to ongoing Act compliance (see Exhibit 6.3). This approach encompasses a broad spectrum of considerations that will help ensure Act compliance. The Path, like any ongoing compliance approach, should be tailored to fit the individual needs of the business.

To help ensure the success of an ongoing compliance program, the following issues should be considered.

Monitoring

The final step of initial compliance discussed in Chapter 4 recommended that companies implement ongoing and continuous monitoring systems since the requirements of Section 302 and Section 404 each require ongoing compliance. Each company must build a monitoring process.

There are basically two types of future state monitoring processes: continuous monitoring and specific testing. A continuous monitoring system is one that is built directly into the significant processes and control activities and occurs with a regular frequency. Specific testing systems are separate reviews that are conducted on particular processes or controls and often are the result of some triggering event. Both types of controls can easily be incorporated into self-assessment programs.

A combination of these monitoring systems should be implemented to provide continuous monitoring and maintenance of internal controls and to

Ongoing Compliance Activities

Step 1. Plan

- Establish compliance steering committee
- Determine who will be in charge of ongoing Act compliance efforts
- Develop actual compliance program planning
- Checkpoint: external auditor considerations
- Step 1 expected outcomes

Step 2. Document

- Documentation
- Checkpoint: documentation standardization
- Gap analysis
- Step 2 expected outcomes

Step 3. Test

- Control testing plan
- Conduct internal testing
- Checkpoint: attestation engagement
- Prepare evidential documentation
- External auditor testing
- Step 3 expected outcomes

Step 4. Remediate

- Close gaps and strengthen internal controls
- Checkpoint: business streamlining opportunities
- Step 4 expected outcomes

Step 5. Report

- Checkpoint: draft certification disclosures
- Management certifications
- External auditor attestation
- Step 5 expected outcomes
- Demonstrated compliance!

Exhibit 6.3 The Path to Ongoing Compliance

ensure remediation efforts are completed in a timely manner. Businesses can take advantage of numerous software applications that have built-in monitoring capabilities or they can implement internal control self-assessments. Any tools that are used to facilitate the process will still be

Ongoing Maintenance and Monitoring

heavily dependent on employee execution. All employees must take responsibility for monitoring and correcting internal control systems.

Internal Control Self-Assessments

When the Committee of Sponsoring Organizations (COSO) first emerged as a framework for evaluating internal controls, many businesses began utilizing internal control self-assessment questionnaires as a technique to drive internal control responsibilities through the organization to the process owners and users. This incited process owners to become more involved in the design and analysis of the continuing effectiveness of the internal control environment for their respective processes.

Internal control self-assessments have many positive attributes:

- They are reasonably inexpensive to develop and implement.
- They involve a large percentage of employees, which increases the probability that weaknesses will be detected.
- They involve the process owners and users, who are the most knowledgeable about specific processes.
- They can facilitate the development of a strong internal control environment, provided that executive management sets the tone from the top.
- They provide a mechanism for detecting control deficiencies and identifying potential process improvements.

Conversely, internal control self-assessments can quickly turn into just another checklist activity after the first year. To ensure that self-assessments are effective for an extended period of time, the business must foster a culture that values both internal control and continuous process improvement and, thus, employees are rewarded for their efforts.

Tone at the Top

The tone of executive management will drive the success of all compliance efforts. If management views compliance as a burden, it will become a burden for all employees and much of the value will be lost. Compliance objectives may still be met, but control breakdowns may occur more fre-

Ongoing Compliance Activities

quently and the opportunity to obtain value from process improvements will be ignored.

Process Owners

The importance of process owners in ongoing Act compliance cannot be overstated. Businesses can hire a team of consultants to design, implement, and test systems of internal control, but they cannot ensure systems are used properly and internal controls are followed. The users and process owners primarily drive the success of processes and internal controls. Keep these employees motivated and compliance processes and systems will be used properly. When controls fail, they will be detected early and corrected.

Training and Education

Employees must receive sufficient training and education to perform their jobs well and successfully fulfill the roles required by Act compliance.

STEP 1: PLAN

This is the critical stage in ongoing Act compliance. While the planning stage may seem boring and tedious, it is the cornerstone of effective ongoing compliance. Extra care and consideration during this stage will provide employees with a clear and precise understanding of their objectives and will go a long way toward making sure that objectives are met on time and within budget. The objective of the Path is not just to comply, but to manage a process that allows for ongoing compliance with the Act.

Establish a Project Steering Committee

Determining who is in charge of ongoing compliance is one of the first actions necessary for effective compliance. While many companies will appoint a specific compliance officer to lead compliance activities, overall responsibility should remain with the board of directors and executive management. One way to ensure such oversight is to establish a steering committee for corporate governance and Act compliance with the designated

Ongoing Maintenance and Monitoring

compliance officer as a standing member and a working group to deal with specific process issues. The steering committee should consist of five to seven senior executives. With this constituency, audit committee involvement can be meaningful and continuous. Steering committee discussions should include policy and standard setting. The steering committee should be a vehicle for rapid decision making to facilitate and not hinder ongoing compliance efforts. Businesses with established steering committees for initial compliance efforts should now make such committees permanent. The steering committee may be responsible for enterprise risk management as well as Act compliance.

Companies should also consider forming a working group to support the efforts of the steering committee. Working groups tend to be tactical in nature, discussing issues at a process level and leading ongoing compliance and corporate governance initiatives. The working group should consist of five to seven employees and should be chaired by the person who is ultimately responsible for Act compliance within the business. A March 2004 survey conducted by Parson Consulting (see Exhibit 6.4) shows that

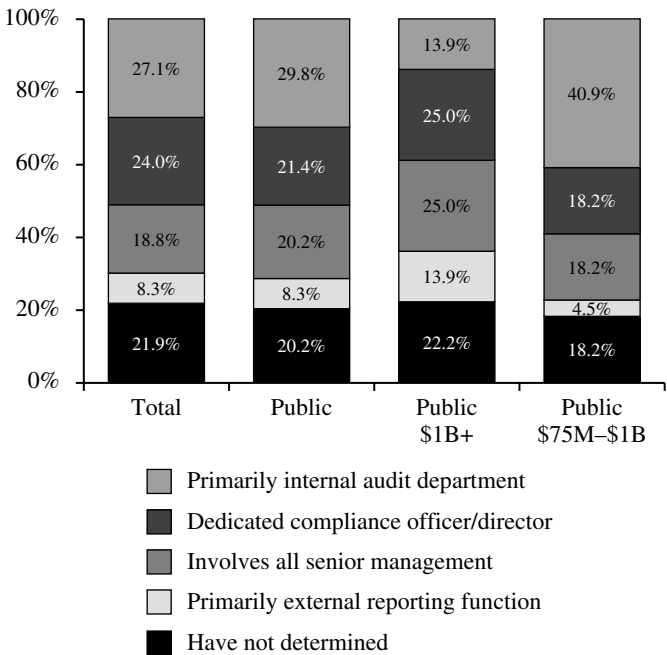


Exhibit 6.4 Who Will Be in Charge of Ongoing Compliance?

Ongoing Compliance Activities

18% to 25% of companies plan to assign a dedicated employee as compliance officer while 24% to 41% of companies plan to assign this responsibility to the chief auditor of the business.

Maintain Ongoing Compliance Planning

Businesses should have generated a detailed project plan during initial compliance. This plan should now be modified to eliminate the one-time efforts of initial compliance such as pilot programs and full documentation requirements. The plan should then be refined to include a current review and risk assessment of the control environment and an assessment of any control deficiencies and remediation activities associated with prior period Act compliance efforts. Companies should then assess risk at three levels: entity risk, business unit risk, and process level risk. Entity risk assessment addresses risk residing at the overall organization level and applies to the entire company being reviewed. Business unit risk assessment addresses risks unique to specific business units within a company. Process level risk assessment addresses the risk at the business process or functional level such as procurement or reporting. The risk assessment of the control environment should also include analyses of software automation opportunities, general controls documentation requirements, outsourced functions, and changes since the prior compliance period. This process should be conducted through interviews with key members of the applicable management team and key process owners. Using a thorough questionnaire can be an effective tool for addressing all relevant subject matters in the risk assessment process.

After completing the risk assessment of the control environment, the compliance plan should be modified to include the risk assessment results.

With these data as a foundation, a specific work plan with well-defined roles and responsibilities should be developed. This plan should also include the specific tasks to be completed, the sequence of tasks to be completed, the expected duration of the tasks, task assignments, expected outcomes from the tasks listed, and critical checkpoint milestones.

Checkpoint: External Auditor Considerations

Following the development of the planning process outcomes, the ongoing compliance program should be developed and prepared for working group

Ongoing Maintenance and Monitoring

approval and communication to the steering committee. Before seeking working group approval, the compliance plan should be checked to ensure that it incorporates external auditor's requirements, expectations, and level of required testing.

Step 1 Expected Outcomes

Expected outcomes include:

- Establishment of a steering committee, working group, and compliance leadership
- A detailed ongoing compliance plan

STEP 2: ONGOING DOCUMENTATION

This step requires the review of existing internal control process documentation and the creation of additional documentation where required. Documentation is not only critical to understanding the control process, but is absolutely necessary to effectively evaluate, remediate, and test the internal control over financial reporting. There are several methods and tools that can be used to document significant processes and the underlying internal controls and procedures. To assist with the documentation phase, a specific example of compliance documentation for a hypothetical company's accounts payable/cash disbursements process is presented in Appendix G. This sample documentation includes:

- Process flowcharts
- Supplemental narrative
- Control matrix
- Segregation of duties
- Process walkthrough
- Control test plan
- Corrective action log

In the documentation phase of ongoing compliance, the creation of detailed process documentation should be limited only to processes that

Ongoing Compliance Activities

have changed since the prior period. While the number of new processes requiring documentation should be few, the extent of the documentation should not be curtailed. The documentation in ongoing compliance should be as comprehensive as that created in the initial compliance efforts and should follow a consistent approach. The documentation process should also include interviews with selected process owners as appropriate. A best practice is to use collaborative business facilitation to run effective process documentation workshops.

After reviewing existing documentation, completing employee interviews, conducting process documentation workshops, and obtaining all other relevant information, current and complete process documentation should be generated for each new or modified significant process and added to the existing documentation database. All documentation should then be finalized except for the control test plan and the corrective action log, which will be finalized after completing the actual process walk-throughs and correcting the control gaps identified during testing.

One last item to be completed during the documentation phase is a COSO matrix that facilitates the comparison of the five COSO control components relating to the COSO control objectives (refer back to Exhibit 1.2) to the control components identified in the documentation of the significant processes. While Act compliance is limited to internal control over financial reporting, all three COSO control objectives should be considered since the financial reporting process may be affected by the efficiency of operations as well as compliance with laws and regulations. To ignore any of the COSO control objectives would be a control deficiency in the Act compliance process. “Accordingly, all controls that could materially affect financial reporting, including controls that focus primarily on the effectiveness and efficiency of operations or compliance with laws and regulations and also have a material effect on the reliability of financial reporting, are a part of internal control over financial reporting.”²

Checkpoint: Documentation Standardization

A critical checkpoint at this phase of ongoing compliance is to determine if the documentation process is consistent throughout the organization. Lack of standardized documentation will not prevent the completion of the project plan, nor will it prevent the attestation of the process of internal control over financial reporting by the external auditor, but it will increase the time

Ongoing Maintenance and Monitoring

and cost associated with both. Inadequate documentation may be considered a control deficiency that could be viewed in certain circumstances to be either a significant deficiency or a material control weakness.³ This risk can be mitigated by implementing standardized documentation requirements for the entire organization as part of the ongoing compliance plan.

Gap Analysis

The last phase of Step 2, documentation, is to actually compare the controls of the newly documented or modified processes to the COSO requirements (and Control Objectives for Information and Related Technology [COBIT], if appropriate), identify control gaps, assess the potential impact of the gaps, define possible solution options, and record the applicable information to the corrective action log. At this point, identified control gaps should be classified as control deficiencies (for a detailed discussion of the definitions of the terms control deficiency, significant deficiency, and material weakness, refer to Chapter 5). Since control testing will not occur until Step 3, the control deficiencies identified through gap analysis will most likely fall under the category of deficiencies of design, but should be further classified as either a significant deficiency or material weakness. Do not forget to identify control gaps resulting from control objectives without a corresponding process control. Control omissions may sometimes be hard to identify, but those that are not addressed by a specific process control will become quite obvious later on. The identification of control omissions further increases the importance of both the documentation process and the development of the COSO control matrix.

Step 2 Expected Outcomes

Expected outcomes include:

- Documentation of significant processes
 - Process flowcharts
 - Supplemental process narratives
 - Control matrix
- Gap analyses with solution options and action plans

STEP 3: TEST

While the gap analysis performed during Step 2 identified control deficiencies, the ultimate effectiveness of internal control over financial reporting will not be determined until the controls over significant processes are appropriately tested. Step 3 in ongoing compliance includes the development of the control testing plan, implementation of the plan, and preparation of evidential matter for use by the external auditor. During the test phase, it is absolutely critical to maintain regular interaction with the external auditor. AS2 sets forth guidance that effectively requires businesses to complete the entire Section 404 reporting and testing process each year for ongoing Act compliance. While business cannot rely on prior period test results, it can utilize prior period testing plans as the basis from which to develop current period plans. If the business already has well-developed testing plans and procedures from the prior period, simply modify such plans to include (1) the risk assessment results developed in Step 1; (2) testing procedures for new and modified processes and controls; and (3) testing procedures for any corrected control gaps identified during documentation. If well developed testing plans do not exist, continue through this section for detailed guidance relating to testing internal controls.

Control Testing Plan

Employees or consultants conducting the control testing should possess a thorough knowledge of the control testing provisions of AS2, including the examples of significant deficiencies and material weaknesses described in Appendix I. Individuals conducting control testing should also consult Complianceweek.com for periodic reports of actual control deficiencies (see Appendix J for actual internal control deficiency disclosures reported on September 8, 2004).

The objective of control testing is to provide an appropriate basis for management to determine the operational effectiveness of the key internal controls identified during the documentation phase. Individuals who are independent of the process or activity being tested must perform control testing. The results from the test procedures will form the basis of, and support, management's assertion on internal control over financial reporting included in annual reports. The external auditor may also consider the

Ongoing Maintenance and Monitoring

results of testing during their attestation of, and report on, management's assessment of internal control over financial reporting.

Appropriate testing procedures include inquiry, observation, inspection, performance of control activities, and examination of evidence necessary to support account balances. Testing also addresses the execution and effectiveness of key internal controls. Controls should be tested at both the entity level as well as the transaction or application level. The entire population of transactions over which a key control is performed forms the basis for selection of the test sample. This includes all significant locations and reporting units.

The following factors should be considered in deciding the extent of testing:

- The degree to which the control is relied upon as a basis for its assertion (the higher the degree of reliance, the more extensively the control should be tested)
- The relative importance of the potential errors that could result if the control is not functioning properly
 - Materiality of the transaction
 - Complexity of the transaction
 - Volume of transactions
 - Frequency of transactions
- The competency of the person performing the control
 - Competence, integrity, and ethics of the employee performing the control
 - Employee's independence from the related processing procedures
 - Degree and adequacy of supervision of the employee
 - Extent of employee turnover
- The effectiveness of internal controls at the entity level
 - Likelihood that a control can be bypassed
 - Potential for management overrides of the control
 - Potential risk of fraud
 - Extent of monitoring activities during the fiscal period
 - Likelihood that a control will operate as intended until year end
- Changes in related processes including the effectiveness of current controls after implementation of changes

Ongoing Compliance Activities

- How often the control is performed
 - Automated control testing—generally test one application for each programmed control for each type of transaction if supported by effective IT general controls
 - Manual control testing is based on frequency of performance
 - Performed many times per day—test at least 25 items
 - Performed daily—test at least 20 items
 - Performed frequently, but less than daily—test 25% of the occurrences, but not less than 25 items
 - Performed weekly—test at least 5 items
 - Performed monthly—test at least 2 items
 - Performed quarterly—test at least 2 items
 - Performed annually—test at least 1 items

Management must consider the fact that conclusions drawn on the basis of limited testing may differ from the conclusions drawn if all items under a particular control are tested.

After determining the basis for testing, a control test plan for each significant process should be developed. The control test plan should include the following:

- Significant process tested
- Company, segment, division, department name, and location of the tested process
- Control number for each control tested
- Reference number (to process flowchart)
- Description of the control tested
- Type of control (either design or operation)
- Supporting documents to be reviewed during testing
- Sample size
- Sample selection procedures

An example of a control test plan is included in the sample documentation package in Appendix G. The external auditor should be consulted prior to the execution of the test plans in order to ensure that the extent of

Ongoing Maintenance and Monitoring

testing is adequate to demonstrate the level of effectiveness required by the external auditor when testing control activities.

Conduct Internal Testing

In this phase of Step 3, the control test plan is executed and the results and/or exceptions are noted. During testing, all noted exceptions must be examined by the nature of the exception, the types of financial misstatement that could potentially occur as a result of the exception, the materiality of the potential misstatement, and the ultimate classification of the exception as a control deficiency, significant deficiency, or material weakness. Once the exception is classified and investigated, it may be necessary to implement corrective measures to mitigate the risk, change the control, or change the process. In any event, it is necessary to maintain thorough documentation of the testing, testing results, and conclusions drawn as a result. Test results should be recorded on the transaction test matrix, which is included in the sample documentation package in Appendix G. The two-page transaction test matrix is cross-referenced with the control test plan to ensure that all testing is accomplished and results are documented. Page 1 of the transaction test matrix records the following:

- Significant process tested
- Company, segment, division, department name, and location of the tested process
- Numerical listing of each individual sample transaction test
- Description of the sampled transaction
- Date of the actual recording of the transaction
- Document reference for the transaction
- Listing of each specific control as numbered on the control testing plan and a yes or no indication of whether the control was effective for the tested transaction
- Written testing observations and comments

Page 2 of the transaction test matrix, which is a summary of observed exceptions, records the following:

- Transaction test number (from page 1)
- Exception type

Ongoing Compliance Activities

- Explanation of the exception
- Whether corrective action is required (yes or no)
- Proposed corrective action or the rationale for no corrective action
- Reference to the logging of the corrective action on the corrective action log
- Overall conclusion on the operation of the controls over the specific significant process
 - Process controls are operating as management intends (yes or no)
 - Process controls are operating as management intends with only minimal exceptions that are explainable and require no corrective action (yes or no)
 - Further testing is required to determine if test results (numerous unexplainable exceptions) are an anomaly (yes or no, with a reference to the additional testing if yes)
 - Significant corrective action is required; documentation package will require modification to reflect implementation of corrective action and process control testing will be reperformed (yes or no)
- Certification of the applicable financial officer

All corrective action required by transaction testing of internal control activities should be recorded on the same corrective action log that was initially generated in the “close gaps and strengthen internal controls” phase. This unified approach to identifying control deficiencies and tracking corrective action is a strong control for verifying that all corrective action is addressed. It also provides an easy to follow audit trail for the external auditor’s examination.

Checkpoint: Attestation Engagement

Verify that the audit committee has finalized the engagement of the external auditor for the internal control over financial reporting attestation and communicated the related scope, timing, and cost. If coordination with the external auditor has been ongoing throughout the implementation, the attestation engagement is most likely finalized. If not, there may not be sufficient time for the external auditor to adequately plan and execute the engagement without incurring significant overtime charges, which will ultimately increase the fees charged for the attestation engagement.

Ongoing Maintenance and Monitoring

Prepare Evidential Documentation

In support of the pending external auditor attestation engagement, begin to assemble the documentation review for delivery to the external auditor. If the testing team was diligent in completing recommended documentation, this information should be sufficient to meet the external auditor needs. Actively engaging the external auditor throughout the ongoing compliance process provides reasonable assurance that the internally generated documentation will be sufficient.

External Auditor Testing

It is now time for the external auditor to begin the attestation review. During external auditor testing, the individuals who performed the internal testing should be coordinating and facilitating the external auditor attestation review. Having conducted the testing, they are in the best position to support the external auditor and coordinate the support efforts across the company. They are also best prepared to address any control deficiencies that may arise from the attestation review. The quick resolution and retesting of identified control deficiencies is critical to completing the attestation process within the deadlines for filing the required annual reports. External auditor-identified control deficiencies should be controlled by the same process used for remediation and implementation of corrective action; however, the control deficiencies must be categorized indicating that they arose from the external auditor's attestation process. Any identified significant deficiencies or material weaknesses must be promptly communicated in writing to the audit committee and copied to the steering committee.

Step 3 Expected Outcomes

Expected outcomes from Step 3 include:

- Executed control test plans
- Completed transaction test matrix
- Update corrective action log
- Written communication of all identified significant deficiencies and material weaknesses to the steering committee and audit committee

Ongoing Compliance Activities

- Inputs for the development of a revised remediation plan, which includes the corrective action required by the control testing
- Audit committee finalization of the engagement of the external auditor for the internal control over financial reporting attestation
- Preparation of evidential documentation in support of the external auditor attestation engagement
- Listing of external auditor-identified control deficiencies if applicable (corrective action should be included in the corrective action log)
- Written and timely communication of all external auditor identified significant deficiencies and material weaknesses to the audit committee

STEP 4: REMEDIATION

The corrective action log should be summarized by significant process in order to create the initial remediation plan. The plan should include, by process, the total number of control deficiencies, total number of significant deficiencies, total number of material weaknesses, individuals responsible for implementing the corrective action, planned date of completion, and the status of the corrective action. These data, along with an overall time line for required corrective action, form the remediation plan. External auditor-identified control deficiencies should be included in the remediation plan, but separately identified to indicate that they arose from the external auditor's attestation process. Other considerations when developing the remediation plan include:

- Identifying individuals responsible for completing each effort
- Prioritizing remediation efforts
- Aligning remediation efforts with the strategic plan
- Aligning remediation efforts with customer needs
- Applying best practices
- Measuring the cost of remediation
- Including process improvements to realize value, where applicable
- Implementing performance metrics
- The need for compensating controls if remediation is not complete by year end

Ongoing Maintenance and Monitoring

After analyzing these issues, the remediation plan should be finalized and presented to the steering committee and audit committee for their consideration and approval. A written communication of all identified significant deficiencies and material weaknesses should be presented to the steering committee and audit committee. Once approved by the audit committee and steering committee, the updated remediation plan should be communicated and implemented. The business may need to operate in a remediation state for a full quarter to ensure the corrective action functions as designed before control retesting can begin.

Step 4 Expected Outcomes

Expected outcomes include:

- Development of the final remediation plan that includes the corrective actions required as a result of control testing as well as those identified by the external auditor
- Steering committee and audit committee presentation of remediation plan
- Steering committee and audit committee review and approval of remediation plan

STEP 5: REPORT

Too many financial managers believe certification and attestation are the ultimate goals of Act compliance. While it is certainly a requirement and a stated goal, it is not the final goal. For Section 302 compliance, all future quarterly and annual financial reports must include a certification executed by the CEO and the CFO while Section 404 compliance mandates that required annual reports include (1) an internal control report stating management's responsibility for internal control and management's assessment of internal controls for the most recent fiscal year; and (2) the external auditor's attestation to, and report on, management's assessments. It is through the process of continuously planning, documenting, testing, and remediation that ongoing compliance is truly achieved.

Ongoing Compliance Activities

Checkpoint: Draft Certification Disclosures

To expedite the final reporting process, the working group should utilize the information generated by the project team to draft the required certification report. The report cannot be finalized until the remediation plan and any additional testing are completed. Preparation of the documents in anticipation of the results of any required retesting will facilitate the final report process, which already comes at a busy time of the year for financial managers. The draft report should be provided to the steering committee and audit committee for review and comment.

Management Certifications

Assuming that the remediation plan and any required control activity retesting is complete, the draft certification disclosures and management's assessment of internal control over financial reporting can be finalized for inclusion in the required annual reports. The final certifications and assessment reports, along with a final report of findings from the project team indicating the status of internal control over financial reporting and the resolution of both the remediation plan and corrective action log, should be presented to the steering committee, audit committee, and certifying executives for final review, modification, and approval.

External Auditor Attestation

The company should receive a copy of the external auditor's attestation to, and report on, the assessment made by company management concerning internal control over financial reporting. The external auditor should communicate the results of the attestation directly to the audit committee and to the steering committee, as well as to executive management.

Step 5 Expected Outcomes

Expected outcomes include:

- Draft management certification and internal control assessment
- Completion of the remediation plan and corrective action log

Ongoing Maintenance and Monitoring

- Final management certifications assessment report presented to the steering committee and audit committee
- Final report on Act compliance presented to the steering committee and audit committee
- Approval of management certifications and assessment report
- Receipt of the external auditors attestation

NOTES

1. Auditing Standard No. 2. An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements, Paragraphs 147–149, effective pursuant to SEC Release no. 34-49884; File No. PCAOB-2004-03, June 17, 2004.
2. *Id.*, paragraph 15.
3. *Id.*, paragraph 45.

AUDIT FUNCTION CONSIDERATIONS

The Sarbanes-Oxley Act has fundamentally changed the roles of the internal auditor and the external auditor. The clear intent of the Act was to change the relationship between companies and their external auditor since it appeared that auditors had lost their independence by providing both consulting services and financial reporting guidance to clients they were auditing. But the Act has also affected the internal audit function, causing many departments to reexamine their roles in light of the need for ongoing compliance. As a result, the roles of both internal auditor and external auditors are changing and will continue to do so as the full impact of the Act is determined and the Public Company Accounting Oversight Board (PCAOB) continues to issue new auditing standards and guidance.

THE ROLE OF THE INTERNAL AUDIT DEPARTMENT

Financial managers must consider the skills, experience, scope, and independence of the internal auditors and the department as a whole when determining exactly what role internal auditing should play in ongoing compliance efforts. The role of the internal auditor was originally focused on attesting to financial matters and assessing internal controls. Over the past 10 years, the department's role has increasingly focused on operational auditing and strategic business issues in an effort to improve performance and demonstrate value to the business. As a result, the focus of internal auditing was skewed more toward operational auditing than internal control over financial reporting. The Institute of Internal Auditors (IIA) Statement of Responsibilities of Internal Auditing defines the objective and scope of internal auditing as follows:

Ongoing Maintenance and Monitoring

Internal auditing is an independent appraisal function established within an organization to examine and evaluate its activities as a service to the organization. The objective of internal auditing is to assist members of the organization in the effective discharge of their responsibilities. To this end, internal auditing furnishes them with analyses, appraisals, recommendations, counsel, and information concerning the activities reviewed. The audit objective includes promoting effective control at reasonable cost. The members of the organization assisted by internal auditing include those in management and the board of directors.

The scope of internal auditing should encompass the examination and evaluation of the adequacy and effectiveness of the organization's system of internal control and the quality of performance in carrying out assigned responsibilities.¹

It is apparent that the scope of the internal audit department today is much greater than just auditing internal control over financial reporting; however, with that change in scope comes a corresponding change in skills. Operational auditing requires a broad knowledge of operating systems and skills as well as consulting approaches. Since reviews are often focused on business processes rather than financial processes, auditors tend to have strong consulting and operational skills rather than traditional audit skills. The move toward operational auditing over the past decade has left many internal audit departments with staff members who have no traditional audit experience or skills. While these auditors can provide value to organizations in the form of operational reviews or technical assistance, they are not necessarily the appropriate individuals for assessing internal control over financial reporting and conducting ongoing Section 404 testing. Therefore, it is imperative that companies first decide what role internal auditing will play in Act compliance, and then evaluate the skills within the department to determine whether resources may need to be added to address both business risks and the requirements of Section 404.

Another key consideration of the role of internal auditing is the independence of the audit function, particularly in conjunction with Act compliance. IIA Statement of Responsibilities of Internal Auditing defines internal auditor independence as follows (see also Appendix I for the full statement):

Internal auditors should be independent of the activities they audit. Internal auditors are independent when they can carry out their work freely and objectively. Independence permits internal auditors to render the

Audit Function Considerations

impartial and unbiased judgments essential to the proper conduct of audits. It is achieved through organizational status and objectivity.

The organizational status of the internal auditing department should be sufficient to permit the accomplishment of its audit responsibilities. The director of the internal auditing department should be responsible to an individual in the organization with sufficient authority and independence to ensure a broad audit coverage, adequate consideration of audit reports, and appropriate action on audit recommendations.

The organizational status of the internal auditing department should be sufficient to permit the accomplishment of its audit responsibilities. The director of the internal auditing department should be responsible to and individual in the organization with sufficient authority to promote independence and to ensure a broad audit coverage, adequate consideration of audit reports, and appropriate action on audit recommendations.

Objectivity is an independent mental attitude that internal auditors should maintain in performing audits. Internal auditors are not to subordinate their judgment on audit matter to that of others. Designing, installing, and operating systems are not audit functions. Also, the drafting of procedures for systems is not an audit function. Performing such activities is presumed to impair audit objectivity.²

Just as external auditors are charged with becoming too close to the companies that they were auditing, many internal audit functions are perceived to have become too close to internal departments in conducting operational reviews. In an effort to demonstrate worth or added value, many internal audit functions have come precariously close to the line between providing audit assessments and guidance and participating in the design of controls, practices, processes, and procedures, which are not audit functions included in the IIA definition of independence.³ The IIA independence definition also states that the “drafting of procedures for systems is not”⁴ an internal audit department function. As the focus of internal audit departments has changed, the independence of the internal audit function appears to have become blurred.

The reporting relationship of the internal audit department is also important to consider. The involvement of internal auditing in ongoing compliance activities may require a change in the reporting relationship of the department. If the internal audit function plays a major role in ongoing compliance and reports to the chief executive officer or chief financial officer, it could be perceived as not truly independent. One solution to this

Ongoing Maintenance and Monitoring

independence issue is to have the internal audit department report directly to the audit committee of the board of directors, as is required by the Act.

The exact role that internal auditing plays in ongoing compliance varies by company and is highly dependent on the skills and availability of the auditors. In general, internal auditing may fulfill the following functions with regard to Act compliance:

- *Process documentation.* Internal auditors in general are skilled in documenting internal process and controls both through narratives and flowcharts. In most cases, process owners do not possess the skills necessary to adequately document internal controls and processes such that the documentation may be used by external auditors in determining the scope of their attestation review.
- *Internal control gap analysis.* Internal auditors with specific financial auditing skills have the expertise to review process documentation, which includes all control points, and ascertain whether or not control gaps exist.
- *Testing.* Internal auditors with traditional auditing training and experience in statistical sampling techniques are the perfect individuals to conduct internal testing of the internal control processes. This is another area where process owners generally lack the requisite skills to adequately perform the function.
- *Guidance on internal controls.* Internal auditors may provide guidance on what are sufficient internal controls as long as they do not actually participate in determining the controls and writing procedures.

According to the IAA definition of independence, internal auditors cannot fulfill the following roles:

- *Draft, develop, or implement internal controls, processes, or procedures.* As soon as the auditors perform any of these roles, they lose their independence and their ability to effectively conduct an audit of such controls, processes, or procedures. Simply having one auditor draft, develop, or implement and another conduct the actual audit will typically not remove the conflict of the department auditing its own work.
- *Process owner.* Internal audit cannot be a process owner and an independent auditor at the same time. While process owners can

Audit Function Considerations

perform self-assessments, they cannot provide independent assurance as to the integrity of internal controls.

- *Remediation.* Again, internal auditors cannot remediate control gaps or deficiencies because testing such remediation efforts would result in auditors reviewing their own work product.

In general, it makes sense for the internal audit department to take an active role in ongoing compliance efforts, but they cannot be involved in the entire process without infringing on auditor independence standards. Internal auditors generally have a strong understanding of the business's control environment and have the skill set to audit internal controls; however, extensive involvement in the process may jeopardize their objectivity or independence, which could lead the external auditors to conclude that a control deficiency exists.

One way in which companies can eliminate most of the risk surrounding the involvement of the internal audit department is to establish a separate function to deal with ongoing Act compliance activities that reports to the ongoing compliance steering committee or directly to the audit committee. By creating this segregation, independence is maintained and you can assure that each function consists of employees with the requisite skills and experience to effectively complete their tasks. This segregation of duties also allows the internal audit department to continue to fully utilize the valuable operational auditing skills it possesses.

Another consideration is to retain third-party consultants to assist with ongoing compliance activities. This approach has the same benefits as separating Act compliance from internal audit activities, except that it will most likely come at a higher dollar cost. The higher cost can be offset by the company's ability to make more rapid progress toward compliance as it develops the appropriate internal staffing, obtains staffing flexibility to deal with peak resource requirements, and incorporates expert advice into its compliance efforts.

Finally, for some companies compliance with the Act may be the catalyst for the creation of the business's first internal audit function. In such cases, it will be extremely important to define the role of the audit department, its reporting relationship, its function in conjunction with ongoing Act compliance activities, and requisite skills of the auditors early on in the development of the audit function. Simply taking a key member of the initial Act compliance team and appointing him or her to lead the internal audit function can be disastrous. It is critical that the audit function be led

Ongoing Maintenance and Monitoring

by someone who not only has proven internal audit skills, but also possesses the ability to create an effective internal audit department that will function at a high level.

THE ROLE OF THE EXTERNAL AUDITOR

Compliance with the Act has had a significant impact on the role of the external auditor. While the Act and subsequent pronouncements from the PCAOB have not changed the external auditor's responsibility for conducting financial statement audits, the effect on how external auditors conduct such audits is extensive. While Section 404 of the Act creates additional work for the external auditor in the form of an attestation review of management's assessment of internal control over financial reporting, it is the Act's provisions in Title I (Public Company Accounting Oversight Board) and Title II (Auditor Independence) that drive the real change in the role of the external auditor. Title II, among other things, establishes a new standard for auditor independence, prohibits external auditors from performing specific nonfinancial statement audit activities, and establishes that external auditors are to be retained by and accountable to the company's audit committee of the board of directors. But Title I's creation of the PCAOB to establish or adopt auditing, quality control, ethics, and independence standards relating to the preparation of audit reports and enforce compliance with the Act arguably has the most impact on the role of the external auditor. A clear understanding of the promulgations of the PCAOB will go a long way toward maintaining an effective working relationship with the external auditor within the new environment of Act compliance.

As a result of the Act and PCAOB pronouncements, external auditors are required to perform an attestation review of management's assessment of internal control over financial reporting in conjunction with a company's financial statements audit. The PCAOB standards and rules make it very clear that the external auditor's attestation is not to be simply a rubber-stamped endorsement of management's report on internal controls, but a critical aspect of assuring the reliability of financial reporting.

The information the external auditor learns as a result of auditing a company's financial statements has a direct and important bearing on the auditor's conclusion about the effectiveness of the company's internal control over financial reporting. Since an internal control audit cannot be separated from a financial statement audit, the PCAOB has concluded that

Audit Function Considerations

an integrated audit approach must be used. An integrated audit accomplishes two separate objectives: (1) to express an opinion on management's assessment of the effectiveness of the company's internal control over financial reporting, and (2) to express an opinion on whether the financial statements are fairly presented.

To support an opinion, the external auditor must obtain evidence about whether internal control over financial reporting is effective. The external auditor obtains this evidence in several ways, including evaluating and testing management's assessment process; evaluating and testing internal control work performed by others (such as internal auditors); and testing the effectiveness of controls.

PCAOB Auditing Standard No. 2 (AS2) provides external auditors with significant flexibility in using the relevant work of highly competent and objective personnel, while also requiring external auditors to obtain—through their own auditing procedures—a meaningful portion of the evidence that supports their opinion. An integral aspect of the external auditor's "own" work must include walkthroughs during each annual audit that traces a transaction from origination through the company's accounting and information systems and financial report preparation processes to ultimately be reported in the company's financial statements.

The auditor must consider other relevant and available information about internal control when evaluating internal control effectiveness. AS2 requires the external auditor to understand the results of procedures performed by others (e.g., internal auditors, other company personnel, and third parties working under the direction of management) on internal control over financial reporting. AS2 also requires the auditor to review all reports issued during the year by the internal auditor that address internal controls over financial reporting and evaluate any internal control deficiencies identified in those reports.

While AS2 requires external auditors to understand the results of procedures performed by others, it does not allow external auditors to rely on the conclusions of others concerning the operational effectiveness of internal controls in forming their opinion. This confusing issue must be clearly understood to help prevent disagreements as to the scope of the external auditor attestation efforts. If a competent and sufficiently independent party prepares documentation, performs test work, and upon the external auditors' review of the work determines it to be adequate and complete, the external auditors may use the work when they conduct their audit work. Theoretically, external auditors gain a higher degree of confidence that

Ongoing Maintenance and Monitoring

management's assessment is thorough and accurate, and therefore may not have to test all of the work prepared by others to ensure the independent party was sufficiently objective and competent. Work prepared by others, even if it is adequate, may not be "counted" toward the work to be performed by the external auditors in areas that are crucial to their attestation. External auditors must form their own opinion about the design and operational effectiveness of internal control over financial reporting and must perform all of their own process walkthroughs so they can base their conclusions, and ultimately their opinion, on their own principle evidence.

The standards of auditor independence have changed significantly in addition to the external auditor's ability to rely upon the work of others. Pursuant to the Securities and Exchange Commission's (SEC's) Rule 2-01 on auditor independence, external auditors' independence is impaired if they audit their own work, including any work on designing or implementing an audit client's internal control system. Additionally, AS2 explicitly prohibits auditors from accepting an engagement to provide an audit client with an internal control-related service that has not been specifically preapproved by the audit committee.

Act compliance calls for a fundamental shift in how companies communicate with their auditors, which has left some finance executives concerned over their external auditor's inability to actively participate in the preparation of the business's quarterly and annual financial statements. The PCAOB recognizes that an auditor and a client must be able to communicate and effectively work together in order to produce accurate information for investors and interested parties. The auditor may keep the client apprised of new and developing accounting standards and technical issues, but cannot advise the client on the implementation of the standards and/or financial statement presentation. This means that the business must either have internal resources to at least apply proper accounting treatment to a transaction or footnote disclosure in their financial statements or retain the services of an additional subject matter expert to provide such guidance.

In regard to interim or draft financial statements, the PCAOB has provided guidance that the business must communicate to the external auditor specifically which figures, tables, and footnote disclosures are not final so that the external auditor does not misinterpret an incomplete section as an incorrect section. Such a misinterpretation could result in the external auditor concluding that a significant deficiency or material weakness exists in the internal control over financial reporting. While the PCAOB does not

Audit Function Considerations

dictate the form of this communication, it is best to converse through written communication.

The key to an effective relationship with the external auditor is to establish clear and open communication. To further alleviate potential issues with external auditors and to ensure maximum cooperation throughout ongoing compliance efforts, businesses should consider the following guiding principles:

- Ensure that the audit partner is effectively engaged in the entire audit and attestation process.
- Involve the external auditor in the ongoing compliance efforts early and often. Build review checkpoints into the process to ensure active participation where appropriate.
- Be very specific when requesting information. Provide draft documents whenever possible and request feedback.
- When submitting draft or interim financial statements, ensure you stipulate in writing:
 - The state of completion
 - The extent of the controls that have or *have not* operated at the time the statements were provided.
 - The purpose for which the draft financial statements were provided
- Conduct face-to-face meetings instead of phone conversations or e-mail exchanges to ensure agreement and the accuracy of the communication.
- Always clarify expectations—both the company's and those of the external auditor.

Because of the significance of the new independence provisions and PCAOB pronouncements, the proper form and level of interaction between companies and their external auditors will continue to evolve until all parties are comfortable with their understanding of the new requirements. The effectiveness and extent of such communications may be somewhat constrained by the external auditor's efforts to remain independent, but such issues may only be short-term concerns. The key to a successful relationship with the external auditor now and in the future is to establish continuous clear and open communication.

SAS 70 REPORTS

Many organizations have pursued initiatives that focus their efforts on the core business. As a result of such efforts, outsourcing of noncore activities such as payroll, information technology, human resources, and benefits administration has become more prevalent. Service agreements for such activities can include the outsourcing of entire functions and business unit operations or specific tasks. Regardless of the extent of a company's reliance on outside service providers, such relationships may complicate management's internal assessment of internal control over financial reporting as well as the external auditor attestation engagement.

In conducting the Section 404 required internal management assessment of internal control over financial reporting, businesses must document and evaluate *all* internal controls deemed significant to the financial reporting process. If service providers are engaged to provide any significant services that may affect the business internal control environment, management must obtain the necessary information from the service organization to determine the operational effectiveness of the service organization's internal controls. AS2 states clearly that when a service provider's "services are part of the company's internal control over financial reporting, management should consider the activities of the service organization in making its assessment of internal control over financial reporting, and the auditor should consider the activities of the service organization in determining the evidence required to support his or her opinion."⁵ The fact that a business utilizes service providers "does not reduce management's responsibility to maintain effective internal control over financial reporting."⁶

Established auditing practices and standards already address two options for obtaining the information necessary for assessing the internal controls of services providers: (1) businesses can conduct an internal audit of the each service provider's internal controls over the outsourced activities (task, functions, or operating units), or (2) they can obtain an SAS 70 service auditor report from the service provider if one is available. Of the two options, obtaining an SAS 70 report is the most likely answer to assessing the internal control of service providers since it is highly unlikely that service providers will allow businesses to conduct internal audits.

What exactly is an SAS 70 audit report? The Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA) issued "Statement on Auditing Standards (SAS) No. 70, Service Organi-

Audit Function Considerations

zations” in April 1992 to provide external auditors with in-depth audit guidance relating to the audit of a third-party service organization. The product of a SAS 70 audit has become known simply as a SAS 70 audit or SAS 70 letter. A SAS 70 audit is an in-depth audit of a service provider’s control activities, which generally include controls over information technology and related processes (for a detailed discussion of SAS 70 audit considerations, refer to the AICPA audit guide titled “Service Organizations, Applying SAS No. 70, As Amended”).

SAS 70 provides for two types of reports (type I and type II) that can be issued by the external auditor providing the review (see Exhibit 7.1). In a type I report, the service provider’s external auditor will express an opinion on (1) whether the service provider’s description of its controls presents fairly, in all material respects, the relevant aspects of the service organization’s controls that had been placed in operation as of a specific date, and (2) whether the controls were suitably designed to achieve specified control objectives. In a type II report, the service provider’s external auditor will express an opinion on the same two items noted in a type I report as well as (3) whether the controls that were tested were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives were achieved during the period specified.

In addition to requiring businesses to consider the activities of service providers in conducting Section 404 internal control assessments, AS2

<i>Report Contents</i>	<i>Type I Report</i>	<i>Type II Report</i>
1. Independent service auditor’s report (e.g., opinion)	Included	Included
2. Service organization’s description of controls	Included	Included
3. Information provided by the independent service auditor; includes a description of the service auditor’s tests of operating effectiveness and the results of those tests	Optional	Included
4. Other information provided by the service organization (e.g., glossary of terms)	Optional	Optional

Exhibit 7.1 SAS 70 Audit Report Types

Ongoing Maintenance and Monitoring

clearly establishes SAS 70 type II as the accepted format that allows management to assess the operating effectiveness of the controls of the service provider.⁷ On the surface, obtaining SAS 70 letters for each service provider and incorporating such reports into the internal assessment of internal controls appears straightforward, but in reality it contains many challenges for businesses.

First, businesses must develop a list of *all* outsourced activities and how such activities relate to the financial statements. This list must then be narrowed to determine whether a SAS 70 letter is required. If a SAS 70 letter is required, the AS2 mandates that the report be a SAS 70 type II. In general, a SAS 70 report is needed if a service provider is processing financial transactions, maintaining records, and/or preparing reports for a client company and the company does not specifically direct the activities and transactions. An example of an outsourced activity requiring a SAS 70 letter is when a bank or financial institution is conducting ongoing investment activities, record keeping, and reporting for a business. Conversely, a SAS letter is not required in the situation where a bank is only processing checking account transactions for a business because this activity is under the instruction of the business and the control environment remains primarily under the control of the business.

The PCAOB staff provided additional guidance for use in determining what types of outsourced activities fall within the structure of a business's internal control over financial reporting and would therefore require a SAS 70 letter. The staff concluded that a service provider's "services are part of the company's information system if they affect any of the following:

- The classes of transactions in the company's operations that are significant to the company's financial statements
- The procedures, both automated and manual, by which the company's transactions are initiated, authorized, recorded, processed, and reported from their incurrence to their inclusion in the financial statements
- The related accounting records, whether electronic or manual, supporting information and specific accounts in the company's financial statements involved in initiating, authorizing, recording, processing, and reporting the company's transactions
- How the company's information system captures other events and conditions that are significant to the financial statements

Audit Function Considerations

- The financial reporting process used to prepare the company's financial statements, including significant accounting estimates and disclosures''⁸

After establishing the list of service providers for which SAS 70 type II letters are required, review this list (and those service providers eliminated from consideration) with the external auditor to reach final agreement. Early in the year for which the management assessment of internal control will apply, request a SAS 70 type II letter from each service provider identified. As part of this request, the service provider should be asked if it can provide a SAS 70 type II letter and whether the letter will be completed in time for the business to assess the report as an integral aspect of its overall assessment of internal control over financial reporting.

If the service provider is unable to provide a SAS 70 letter or the SAS 70 letter will not be available in time for the business to complete management's assessment, the external auditor should be consulted to determine the best course of action in the short term under the circumstances. In the long term, service providers that are unable or refuse to provide SAS 70 reports may have to be audited or the outsourced activity may need to be transitioned long term to a different service provider who can provide a SAS 70 letter. This determination must be made after consultation with the external auditor.

One additional consideration regarding SAS 70 reports is the period for which the service provider's SAS 70 report applies. If management's assessment of internal control is for the period ending December 31, 2006, and the service provider's SAS 70 letter is for the period ending March 31, 2006, the SAS 70 report may not be sufficient to assure management of the adequacy of the service provider's internal control or to allow the external auditor to conclude that no deficiencies exist. The PCAOB concluded the following in response to questions about time gaps between management's assessment and a service provider's SAS 70 letter:

Paragraph B25 through B27 [of AS2 Appendix B] provide directions when a significant period of time has elapsed between the time period covered by the tests of controls in the service auditor's report and the date of management's assessment. These directions do not establish any "bright lines." In other words, application of the directions does not result in a precise answer as to whether a service auditor's report issued more than six months prior to the date of management's assessment is not current enough to provide any evidence. Rather, these directions state that,

Ongoing Maintenance and Monitoring

when a significant period of time has elapsed between the time period covered by the tests of controls in the service auditor's report and the date of management's assessment, additional procedures should be performed.

Paragraph B26 provides directions to the auditor in determining whether to obtain additional evidence about operating effectiveness of controls at the service organization. The auditor's procedures to obtain additional evidence will typically be more extensive the longer the period of time that has elapsed between the time period covered by the service auditor's report and the date of management's assessment. Also those auditor's procedures will vary depending on the importance of the controls at the service organization to management's assessment and on the level of interaction between the company's controls and the controls at the service organization.⁹

In other words, if the period gap between the service provider's SAS 70 report and management's assessment period is greater than six months, the external auditor will require some additional audit procedures. In cases where such a period gap exists, businesses should ask their service providers to provide at least semiannual SAS 70 reports, which would result in management's assessment being covered by multiple reports. Many larger service providers are already considering this solution to address the period gap issue. While the cost of additional, or interim, SAS 70 reports will likely be passed along to clients, the impact to any one business will be directly proportional to the number of clients served by the service provider. Again, if the service provider is unwilling or not able to provide interim SAS 70 reports and refuses to allow the business to conduct its own audit, the business should consider outsourcing the activity with another service provider. These considerations must also be assessed when evaluating the engagement of all future service providers.

NOTES

1. The Institute of Internal Auditors, Statement of Responsibilities of Internal Audit, 1990.
2. *Id.*
3. *Id.*
4. *Id.*
5. Auditing Standard No. 2. An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial State-

Audit Function Considerations

ments, Appendix B, effective pursuant to SEC Release no. 34-49884; File No. PCAOB-2004-03, June 17, 2004.

6. *Id.*
7. *Id.*
8. PCAOB Staff Questions and Answers Related to Auditing Internal Controls Over Financial Reporting, pages 21–22, June 23, 2004.
9. *Id.*, page 23.

OTHER ONGOING COMPLIANCE ISSUES

There are various issues that require special consideration and diligence before a company's ongoing compliance efforts can be finalized. Such issues include software applications to assist with compliance efforts, information technology (IT) system implementations, mergers and acquisitions, due diligence, acquisition integration, and the size of the business. Each of these areas requires careful consideration as to their impact on the internal control environment. Due to the differences in control environments among businesses, the same circumstance could cause divergent results at different companies.

SOFTWARE APPLICATIONS TO ASSIST WITH COMPLIANCE EFFORTS

Many companies opted not to purchase compliance-related software to manage the initial compliance effort, delaying the decision until the business was in a better position to determine ongoing needs, assess the Act requirements, and evaluate evolving software applications.

There are many compliance software application products available to businesses. Such applications can be divided into three basic types: process documentation applications, act compliance applications, and overall enterprise risk management applications.

Specific process applications are free-standing existing applications that were not specifically designed to address Act compliance, but are well suited to address particular aspects of compliance. These applications are generally inexpensive, relatively easy and quick to implement, but lack the ability to fully integrate compliance efforts. An example of a specific process application would be any software design to map a control process.

Ongoing Maintenance and Monitoring

Act compliance applications are broad compliance applications that attempt to fully integrate Act compliance. These products are specifically designed to meet the requirements of Act compliance, and are more expensive and require more time to implement than specific process applications. Such products may go well beyond the needs of the financial manager by addressing human resources and legal compliance issues in addition to Sections 302 and 404 compliance. Generally speaking, such applications are more encompassing than specific process applications.

Enterprise risk management applications are the broadest applications of the three. Their focus is not limited to a single aspect of compliance or simply to Act compliance. Such applications are designed to allow companies to assess and manage risk across the entire organization, which includes Act compliance, corporate governance, and other aspects of enterprise risk management. Enterprise risk management applications have existed for many years, but are only now beginning to integrate Act compliance into their overall framework for risk management. Such applications are the most expensive and time consuming of the three options to implement. They can be quite complex but provide an excellent tool for managing complex, diverse, multiplant operations.

Each of these applications has advantages and disadvantages that must be weighed against the business objectives and individualized Act compliance plans. Technology tools can play a vital role in ongoing Act compliance, but deciding which tool or combination of tools to use is critical to the success of ongoing compliance efforts and should not be undertaken without properly examining the key aspects of the overall compliance plan and the future state and strategy of the business. A poor decision will result in increased cost and wasted time and effort.

To prevent such an occurrence, there are several considerations that businesses should examine before they purchase Act compliance software. Recognizing that numerous software vendors simply relabeled existing software applications after adding specific Act compliance features in a rush to meet the void of dedicated Act compliance software products, many companies are taking a long-term approach to compliance by utilizing a combination of existing specific purpose applications and home-grown applications until more comprehensive applications have matured and proven their value. The following are key considerations for selecting software applications:

- *Business strategy.* Deciding which application to purchase must first and foremost be driven by the business and compliance strategy of

Other Ongoing Compliance Issues

the company. If the strategy of the business is to utilize Act compliance to drive process improvement initiatives, it is imperative that the software application facilitates this process as opposed to creating system barriers. It does not matter whether the application software is based on the latest technology if the technology does not meet the needs of the business.

- *Process owner involvement.* It is important to directly involve process owners in the selection process to ensure implementation success. The appropriate software application will facilitate the completion of their jobs; the wrong choice will hurt the compliance effort.
- *Selection criteria.* Selection criteria is based heavily on the needs of the business, the desires of the process owners, the capabilities of information technology, and the influence of external auditors. Selection criteria include:
 - The extent of corporate governance to be included in the application scope
 - The extent of Act compliance to be included in the application scope
 - Central data repository, search, and retrieval capabilities
 - Process work flow control
 - Monitoring capabilities
 - Facilitation and documentation of risk assessment, testing, and remediation
 - Facilitation of internal self-assessment efforts
 - Built-in version controls
 - Security and access controls including remote access for external auditors
 - Electronic sign-off functionality
 - Audit trail documentation and traceability
 - Ability to customize input fields, reports, and certification templates
 - Ease in creating effective flowcharts and other process documents
- *Implementation costs.* Implementation costs should include the application software, licensing fees, hardware requirements, implementation time and expense, training costs, and customization efforts.
- *Relationship to overall enterprise risk management process.* The business's overall approach to enterprise risk management will drive the software selection. If the approach is fragmented, specific

Ongoing Maintenance and Monitoring

process applications may work best. If the approach is coordinated across the entire enterprise, a broad-based enterprise risk management application may be the appropriate choice.

- *Ability to utilize full capability of the application software.* The rapid advancement of technology has resulted in applications with extensive built-in capabilities and functionalities. A disadvantage to this is that too many businesses are unable to fully utilize the capabilities or functionalities due to poor planning and design, a lack of effective training, limitations of existing technologies of the business, or time constraints. This leads to an underutilization of the application and wasted time and resources.
- *The flexibility of underlying application platform.* Underlying application platforms may be rigid and finite, requiring additional time and forethought in the planning stage to ensure compatibility with existing systems.

Act compliance software applications are not the “silver bullets” for Act compliance. They are simply tools to facilitate the process. All may be helpful and valuable when utilized appropriately, but they require foresight, planning, design, setup, and understanding. They will not perform documentation. They will not perform process improvement. They will not perform process testing. And they will not implement remediation. But they may facilitate the compliance process. They also may facilitate the external auditor attestation process by providing the external auditor with a clear and well-documented audit trail of the business’s compliance activity. While the external auditor is not permitted to rely on the results of client work, they may utilize this work in determining the scope of their efforts. The ability to provide access to a database that clearly documents Act compliance activities will strengthen the external auditor’s perception of the internal control environment.

INFORMATION TECHNOLOGY SYSTEM IMPLEMENTATIONS

Businesses that are selecting new IT systems will need to consider the appropriateness of controls built into the software applications. This was a consideration before Sarbanes-Oxley and it is even more important in the new Act compliance environment. The timing of new system implementations also must be taken into account as it can directly impact manage-

Other Ongoing Compliance Issues

ment's assessment and the external audit attestation of internal control over financial reporting. Production date, which system to test (old, new, or both), and whether there is adequate time to perform testing are all key factors to consider. The Public Company Accounting Oversight Board (PCAOB) staff addressed the issues of testing systems close to year end in the following excerpt from their statement issued June 23, 2004:

To audit internal control over financial reporting, the auditor will need to test controls over the new system. Paragraphs 147–149 of Auditing Standard No. 2 provide relevant directions to the auditor in this situation. Those paragraphs state that the auditor's opinion on whether management's assessment of the effectiveness of internal control over financial reporting is fairly stated relates to the effectiveness of the company's internal control over financial reporting as of a *point in time*. Furthermore, Section 404(a) of the Act requires that this assessment be as of the end of the issuer's most recent fiscal year. Because controls over the *new* system, which significantly affect the processing of transactions for significant accounts, are the controls that are operating as of the date of management's assessment, the auditor should test controls over the new system.

Although the auditor would not be required to test controls over the *old* system to have sufficient evidence to support his or her opinion on management's assessment of the effectiveness of internal control over financial reporting as of the end of the issuer's fiscal year, the old system is relevant to the audit of the financial statements. In the audit of the financial statements, the auditor should have an understanding of the internal control over financial reporting, which includes the old system. Additionally, to assess control risk for specific financial statement assertions at less than the maximum, the auditor is required to obtain evidence that the relevant controls operated effectively during the *entire period* upon which the auditor plans to place reliance on those controls. Paragraphs 150 and 151 of Auditing Standard No. 2 [AS2] provide relevant directions to the auditor in this situation.¹

In other words, since management's assessment is meant to report on internal control at a specific point in time, the assessment must include testing of the new system and not the old system. However, since the old system is relevant to the overall production of financial statements, the external auditor is required to obtain evidence that the applicable internal controls operated properly during the entire period (fiscal year) for which the external auditor plans to place reliance upon the internal controls. Thus, the business must test the new system and external auditors must test both

Ongoing Maintenance and Monitoring

the new and the old system. While management is required to test only the new system, it may be prudent for the company to conduct limited testing of the old system to ensure the integrity of the financial audit.

Because management is required to test the new controls as part of their internal assessment, the timing of the system implementation “go live” date is critical. If the go live date is late in the year, there may not be sufficient time to perform adequate testing let alone remediate any control deficiencies that may be identified. For Section 302, certifications simply disclosing the implementation efforts should be sufficient.

MERGERS AND ACQUISITIONS

Mergers and acquisitions have always posed issues for companies. Act compliance makes the issues a little more complicated. Acquisitions made during a fiscal year may be, but are not required to be, excluded from the same year’s management assessment and external auditor’s attestation of internal control over financial reporting. This grace period allows the acquiring company or the newly merged organization time to integrate systems, and evaluate, test, and mitigate controls before inclusion in management’s internal assessment. This exclusion is allowed for one fiscal year only, and the business is required to disclose the exclusion, the identity of the excluded business, and the significance of the excluded business to the consolidated financial statements. Since an acquisition may represent a material change in internal control, companies may be required to disclose merger activity pursuant to both Section 302 and Section 404 of the Act.

As part of the acquisition consideration and due diligence processes, businesses should also consider the adequacy of the target acquisition’s control environment, initial compliance efforts if the target is a private or foreign company, and its effectiveness of internal controls. Companies must also consider the timing of review, testing, and remediation as well as the impact Act compliance will have on the integration process.

BUSINESS SIZE

There are two primary issues to examine when considering business size in relation to ongoing compliance. The first is the actual size of the organization. The second is the number of locations or business units within the company.

Other Ongoing Compliance Issues

In general, smaller businesses will not have many of the formal control processes or mechanisms of their larger business counterparts. As such, financial managers will have a more active and visible role in compliance activities and will be able to directly impact the control environment, encouraging employees to adopt new compliance policies and procedures. Financial managers are also in strong positions to mitigate some of the segregation of duties that is often present in smaller businesses.

Larger businesses with multiple locations or operating units can find guidance on which locations and processes within those locations need to be included in compliance testing in paragraphs 1 through 17 of Appendix H (AS2 Control Testing Provisions). In general, AS2 outlines provisions for the testing of a “large portion” of a company’s operations. Unfortunately, AS2 fails to provide specific guidance as to what constitutes a “large portion” and leaves this to the individual auditor’s (either internal or external) professional judgment. The PCAOB document dated June 23, 2004, provides clarification on AS2 multiplant compliance issues and guidance on the scope of testing at such multiplant businesses. Specific details from the PCAOB document on defining a “large portion,” sampling strategies, and scope limitations are as follows:

Multi-Location Issues

Q16. Paragraph 87 of Auditing Standard No. 2 states: Appendix B, paragraphs B1 through B17, provides additional direction to the auditor in determining which controls to test when a company has multiple locations or business units. In these circumstances, the auditor should determine significant accounts and their relevant assertions, significant processes, and major classes of transactions based on those that are relevant and significant to the consolidated financial statements. Having made those determinations in relation to the consolidated financial statements, the auditor should then apply the directions in Appendix B.

Paragraph B4 states: Because of the importance of financially significant locations or business units, the auditor should evaluate management’s documentation of and perform tests of controls over all relevant assertions related to significant accounts and disclosures at each financially significant location or business unit, as discussed in paragraphs 83 through 105 [of the standard].

Does the combination of these directions mean that, for example, if the auditor determines that accounts receivable is a significant account to the consolidated financial statements, the auditor should test controls over all relevant assertions over accounts receivable at every financially

Ongoing Maintenance and Monitoring

significant location or business unit, even if accounts receivable at a particular financially significant location is immaterial?

A16. No. The combination of these directions means that the auditor should determine significant accounts and their relevant assertions based on the consolidated financial statements and perform tests of controls over all relevant assertions related to those significant accounts at each financially significant location or business unit for which the selected accounts are material at the account level. Therefore, the auditor need not test controls over all relevant assertions for a significant account at a financially significant location where the significant account is immaterial. However, if accounts receivable at a location or business unit that is not otherwise considered financially significant represents a risk of material misstatement to the consolidated financial statements, the auditor should test controls over all relevant assertions for accounts receivable at that location. This direction is consistent with the directions in paragraph B6 addressing locations or business units that involve specific risks.

Q17. The multi-location guidance in Appendix B of Auditing Standard No. 2 states that the auditor should test controls over a “large portion” of the company’s operations and financial position. Many auditors are referring to specific percentages that represent coverage over a “large portion” of the company’s operations and financial position, such as 60 percent or 75 percent. Are these percentages set in Auditing Standard No. 2?

A17. No. Auditing Standard No. 2 does not establish specific percentages that would achieve this level of testing. During the comment period on the proposed standard for the audit of internal control over financial reporting, several commentators suggested that the standard should provide more specific directions regarding the evaluation of whether controls over a “large portion” of the company’s operations and financial position had been tested, including establishing specific percentages. The Board decided that balancing auditor judgment with the consistency that would be enforced by increased specificity would be best served by this direction remaining “principles-based.” Therefore, Auditing Standard No. 2 leaves to the auditor’s judgment the determination of what exactly constitutes a “large portion.”

Additionally, the Note to paragraph B11 states that, “the evaluation of whether controls over a large portion of the company’s operations or financial position have been tested should be made at the overall level, not at the individual significant account level.” For example, if an auditor believes that he or she should test controls over x percent of some measure, that auditor should evaluate whether he or she had tested controls over x percent of the company’s consolidated operations or financial position (e.g., x percent of total assets or x percent of revenues) and not

Other Ongoing Compliance Issues

x percent of each individual significant account.

Q18. Is any type of sampling strategy accommodated by the direction to test controls over “a large portion” of financial position or operations?

A18. Yes. The directions in paragraph B11 of Auditing Standard No. 2 that the auditor should test controls over a large portion of the company’s operations or financial position are intended as a fail-safe to ensure that every audit of internal control over financial reporting is supported by sufficient evidence. In no case should the auditor find that, in following the directions in paragraphs B1-B10, the auditor could merely test company-level controls without also testing controls over all relevant assertions related to significant accounts and disclosures.

The direction to test controls over a large portion of financial position or operations is easily satisfied at companies in which the auditor’s testing of individual financially significant locations or business units clearly covers a large portion. At these types of entities and others, the type of judgment discussed in Q17 in which an auditor determines that he or she should test controls over 60 percent or 75 percent of the company’s financial position or operations are readily satisfied. However, in circumstances in which a company has a very large number of individually insignificant locations or business units, testing controls over 60 percent or 75 percent of the company’s financial position or operations may result in an extensive amount of work, in which the auditor would test controls over hundreds and even thousands of individual locations to reach that type of percentage target. In circumstances in which a company has a very large number of individually insignificant locations or business units and management asserts to the auditor that controls have been documented and are effective at all locations or business units, the auditor may satisfy the directions in paragraph B11 by testing a representative sample of the company’s locations or business units.

The auditor may select the representative sample either statistically or non-statistically. However, the locations or business units should be selected in such a way that the sample is expected to be representative of the entire population. Also, particularly in the case of a non-statistical sample, the auditor’s sampling will be based on the expectation of no, or very few, control testing exceptions. In such circumstances, because of the nature of the sample and the control testing involved, the auditor will not have an accurate basis upon which to extrapolate an error or exception rate that is more than negligible. Furthermore, the existence of testing exceptions would not support management’s assertion that controls had been documented and were effective at all locations or business units.

Therefore, if the auditor elects to use a representative sample in these circumstances and encounters testing exceptions within the sample that

Ongoing Maintenance and Monitoring

exceed a negligible rate, the auditor might decide that testing controls over a very large number of individual locations or business units is necessary to adequately support his or her opinion.

Q19. Paragraphs B16 and B17 of Auditing Standard No. 2 provide direction to the auditor in situations in which the SEC allows management to limit its assessment of internal control over financial reporting by excluding certain entities. The SEC staff's guidance, *Office of the Chief Accountant and Division of Corporation Finance: Management's Report on Internal Control Over Financial Reporting and Disclosure in Exchange Act Periodic Reports, Frequently Asked Questions*, dated June 23, 2004, discusses such situations in Questions 1 and 3. However, that document also instructs management to refer in its report on internal control over financial reporting to disclosure in its Form 10-K or Form 10-KSB regarding the scope of management's assessment and any entity excluded from the scope. How does this disclosure by management in its report affect the directions in Auditing Standard No. 2 that instruct the auditor, in these situations, to report without reference to the limitation in scope?

A19. In these situations, the auditor's opinion would not be affected by a scope limitation. However, the auditor should include, either in an additional explanatory paragraph or as part of the scope paragraph in his or her report, a disclosure similar to management's regarding the exclusion of an entity from the scope of both management's assessment and the auditor's audit of internal control over financial reporting.²

NOTES

1. PCAOB Staff Questions and Answers Related to Auditing Internal Controls Over Financial Reporting, pages 4–5, June 23, 2004.
2. *Id.*, pages 14–17.

PART THREE

BEYOND COMPLIANCE

PROCESS IMPROVEMENT CONSIDERATIONS

Simply complying with the rules is not enough. [Companies] should, as I have said before, make this approach part of their . . . DNA. For companies that take this approach, most of the major concerns about compliance disappear. Moreover, if companies view the new laws as opportunities—opportunities to improve internal controls, improve the performance of the board, and improve their public reporting—they will ultimately be better run, more transparent, and therefore more attractive to investors.

—William Donaldson, SEC Chairman, at the
National Press Club on July 30, 2003

It is hard to argue with Mr. Donaldson's logic whether you believe the Sarbanes-Oxley Act of 2002 is Congress's overreaction to a few isolated instances of corporate fraud or a necessary enactment of law to control a lax corporate environment. The Act is law, and affected companies must comply. The implementation method can however, have a very positive impact on businesses if they make compliance, as Mr. Donaldson says, a "part of their . . . DNA" or corporate culture.

IMPLEMENTATION PHILOSOPHIES

While there are numerous implementation philosophies, they can generally be classified in four categories:

1. Unnecessary burden approach
2. Necessary cost of doing business approach
3. Internal control culture approach
4. Cultural change and process approach

Beyond Compliance

The approach a company takes and Act-compliance implementation success will be driven primarily by the board of directors and executive management and secondarily by market forces and company employees. While market forces and employees can affect the business's focus on Act compliance, they are only secondary drivers because of the time it takes for these factors to produce change.

"Tone at the top" can be an overused cliché when discussing Act compliance, but it is the most significant driver of compliance success. The board and executive management set the tone, good or bad, that will determine how employees view Act compliance. A positive tone at the top can transform the attitude from, "we don't want to comply, but it's the law so we have to" to "yes it's the law, but we will embrace compliance because it will ultimately make us a more efficient and effective business."

Unnecessary Burden Approach

Companies will adopt the unnecessary burden approach when executive management simply believes Act compliance is an "unnecessary burden" based on an overreaction by Congress. The overriding belief here is that the events at companies like Enron and WorldCom were isolated issues and all companies are being punished because of the sins of the few. While this may be correct, the fact is that the Act is law and they must comply. By fighting compliance, executive management is saying it is not important to them, which will drive employees to the same conclusion and attitude. Such companies may be setting themselves up for a failed compliance implementation, which could lead to control deficiencies, false certification, negative attestation audits, and potential fines and penalties. Fortunately, a 2004 PricewaterhouseCoopers survey indicates that only 7% of respondents indicated that their board and executive management believe Act compliance is an unnecessary burden (see Exhibit 9.1).¹ Unfortunately, 7% may be too many.

Necessary Cost of Doing Business Approach

These companies believe that Act compliance, right or wrong, is simply another cost of doing business. The Act has created a set of compliance rules similar to Securities and Exchange Commission (SEC), Internal Revenue Service, or Occupational Safety and Health Administration requirements. Executive management recognizes the reality and importance of

Process Improvement Considerations

Compliance with Sarbanes-Oxley

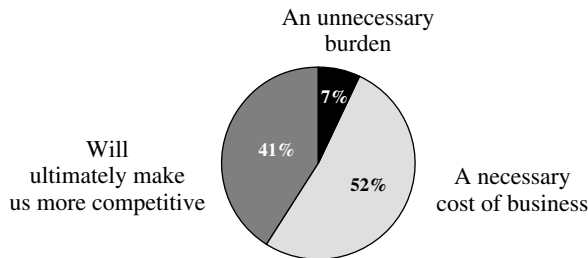


Exhibit 9.1 Predominant Views of Senior Management and Board Regarding Compliance with Sarbanes-Oxley

Act compliance and will dedicate the time and resources necessary to fully comply with the Act and related SEC and Public Company Accounting Oversight Board (PCAOB) pronouncements. These companies will plan their compliance activities, document their systems and controls, test their controls for adequacy, remediate identified control gaps or deficiencies, perform management's assessment of internal controls, and report and certify as required, spending a great deal of time and money to do so. But they will not specifically leverage the information developed in the compliance effort for potential gain. As indicated in the opinion of SEC Chairman Donaldson, "Simply complying with the rule is not enough." It is enough for compliance with the Act, but in Mr. Donaldson's view "opportunities to improve internal controls, improve the performance of the board, and improve their public reporting" are left unfulfilled with this approach. In the aforementioned PricewaterhouseCoopers survey, 52% of respondents indicated that their board and executive management believe Act compliance is a necessary cost of doing business.²

Internal Control Culture Approach

In the necessary cost of doing business approach, executive management recognizes the reality and importance of Act compliance and will dedicate the time and resources necessary to fully comply with the Act and related SEC and PCAOB pronouncements. The difference between this approach and the necessary cost of doing business approach is that executive management recognizes a competitive advantage to going beyond mere

Beyond Compliance

compliance and embracing a strong system of internal control. These companies will still plan, document, test, remediate, report, and certify, but they will do so while looking for ways to improve internal control.

Under this approach, companies will begin by either affirming the existing culture or implementing change that addresses the need for strong internal controls. Creating a cultural shift will refocus compliance efforts on improving internal control, not merely determining whether the internal controls are adequate. The data generated in the process will be used to strengthen and simplify internal controls, as well as to eliminate potential redundancies and inconsistencies resulting from more cost-effective and efficient internal control systems. Chairman Donaldson summarized it well when he said, “If companies view the new laws as opportunities—opportunities to improve internal controls, improve the performance of the board, and improve their public reporting—they will ultimately be better run, more transparent, and therefore more attractive to investors.” While he is correct, companies that take the internal control culture approach to Act compliance are still not fully capitalizing on the knowledge obtained from Act compliance initiatives. This leads us to the fourth approach.

Cultural Change and Process Approach

This approach uses the culture shift in the internal control culture approach as the foundation for further changes within the business. Executive management applying the cultural change and process approach believe the company must go beyond simply focusing on strong internal controls to continually assess, reassess, modify, change, and improve business processes. The process improvement technique chosen—continuous process improvement, six sigma, total quality management, or balance scorecard—is not of primary importance. The key is leveraging the data and knowledge gained from compliance efforts to drive process improvement throughout the business.

Regardless of the size of the business, a significant percentage of revenue is going to be spent on complying with the Act. Some of these expenses, such as internal testing and the external auditor attestation reviews, have little derived benefit toward improving the business. (This does not in any way devalue their benefit to the company. It simply means testing and attestation provide little value in process improvement.) But the expense associated with process mapping and documentation can be leveraged to actually create a positive return on investment from Act compliance expen-

Process Improvement Considerations

ditures. The Culture and Process Approach encourages process owners to use Act compliance initiatives to not only drive process improvement, but also integrate Act compliance and existing process improvement initiatives in the areas of planning, documentation, and implementation to further leverage compliance costs. In other words, they improve the process of process improvement.

PROCESS IMPROVEMENT

The overwhelming task of initial compliance forced many companies to postpone integrating process improvement into their compliance efforts. Emerging from initial compliance efforts, most companies will have a complete catalog of internal controls and processes that are relevant to internal control over financial reporting. But more importantly, they will have documented how each of these processes actually works through process maps, flowcharts, and narratives. This documentation and in-depth understanding provides a foundation for reducing the costs of internal control and creating value from the Act compliance efforts. Process improvement is a natural extension to Act compliance because it not only ensures that businesses capitalize on the knowledge obtained, but also creates the opportunity to realize a return on the investment made in initial compliance.

Continuous business process improvement helps make good businesses great. As author, teacher, and leadership consultant Jim Collins states in his book *Good to Great: Why Some Companies Make the Leap . . . And Others Don't*:

To go from good to great requires transcending the curse of competence. It requires the discipline to say, “just because we are good at it—just because we’re making money and generating growth—does not necessarily mean we can become the best at it.” The good-to-great companies understood that doing what you are good at will only make you good; focusing solely on what you can potentially do better than any other organization is the only path to greatness.³

This good to great mentality must flow from a company’s vision down to each process within a business. Great companies are relentlessly driven to not settle for good, but to be great in everything they do. For the accounts payable manager who is not directly involved in the products or services of a company, it means continually looking for ways to make the

Beyond Compliance

process faster, more efficient, more cost effective, easier to use, and more customer centric. In this way, the accounts payable manager helps to make the company great. Apply this across the board to all process owners, and processes and businesses can use Act compliance as a catalyst for process improvement and transcend “the curse of competence.”⁴

Finance managers can drive process improvement today through the following four steps.

Step 1. Identify the Business Strategy and Communicate It throughout the Finance Organization

Sarbanes-Oxley change initiatives should meet short-term goals and deliver long-term value. The financial objectives of the typical business are a combination of liquidity and working capital optimization, profitability, and growth goals centered on a core product or service. The finance manager should understand the strategic goals of executive management and make sure the entire finance team can articulate those objectives and incorporate them into their everyday activities. Consider the risk implications of the business strategy and counsel management accordingly.

Step 2. Develop a Finance Strategy to Support the Business Strategy

Reevaluate existing key performance indicators and metrics to include crucial Sarbanes-Oxley processes. Identify internal and external stakeholders and the information they need to make insightful decisions. Define, develop, and deploy measurements to satisfy information objectives such as key performance indicators and balanced scorecards as well as benchmark against industry leaders and key competitors in order to establish a performance baseline. Then set goals and define a plan to achieve them. Don’t settle for good; instead strive for great.

Step 3. Generate a Capacity to Provide Analytical and Consultative Services

Remove non-value added processes that were identified during Act compliance documentation. Develop an analytical and consultative capacity within the finance function. This competency is critical to transformation.

Process Improvement Considerations

Measure your own processes. Simplify, streamline, and concentrate transaction and reporting procedures through shared services, outsourcing, and accelerated close methodologies.

Step 4. Leverage Technology to Deliver and Distribute Results

Avoid manual workarounds and reduce the cost of ongoing compliance through technology. Use technology as a key enabler to transformation, but not as the transformation itself. Leverage the capabilities of enterprise resource planning system(s) and integrate wherever practical. Eliminate spreadsheets as a focal point of the reporting process by implementing consolidation and reporting packages. Consider business intelligence and Web-based distribution applications to improve the timeliness and accessibility of critical information.

Other considerations for the financial manager include the following:⁵

- *Take a broad view of functions and processes.* The intent is not to create financial employees who are narrowly focused on their jobs, but instead are motivated to serve the customer, both internal and external. With this focus, there are no sacred cows. All practices and processes are subject to change at any time to achieve the goals of the business first and subsequently the finance department (this assumes no violations of SEC rules, generally accepted accounting principles, etc.).
- *Make processes, problems, and issues visible.* The more people who are aware of processes and surrounding issues, the more likely those processes and issues are to be adequately addressed through process improvement. Great companies do not hide their problems, they improve them.
- *Keep it simple.* Most businesses recognize the value in keeping things simple, but few actually follow such advice. Too often complexity leads to unresolved problems. Not all problems have simple solutions, but many great solutions are simple or are composed of a series of simple solutions.
- *Improve processes before buying new equipment or technology.* All too often in today's environment, businesses rush to a technological fix to process improvement when there are nontechnological solutions or modifications to existing systems can be made. Look first

Beyond Compliance

for obvious solutions within the existing environment. Process improvement is often moved forward by continually rethinking various aspects of a business.

- *Maintain flexibility.* Rigid systems and processes typically produce rigid businesses. This does not mean that the environment should be so loose that internal controls are lax and easily circumvented. Instead, build the capability to react to change and have multiple ways to react to change.

After considering these points, ask yourself the following questions:

- Are you automating manual activities?
- What impact would automation have on productivity?
- Have data process standards been established?
- Are non-value added tasks identified?
- Is employee compensation aligned with business drivers?
- Are business activities and efforts aligned with client perceived value?
- Is there a business case for each process improvement?
- What mechanisms are in place to measure process improvements?
- Are process improvement opportunities prioritized by business impact and level of complexity (see Exhibit 6.1, page 93)?

While these questions and considerations are written with the financial manager in mind, they can be easily applied to other processes and functions, as well as the business as a whole. There are other considerations that businesses should examine when implementing business process improvement. The following items should be applied at the business level, but can be modified for application at the functional and process level:

- Engage organizational leadership to champion change that is in alignment with business strategy.
- Assess overall readiness for change and determine the magnitude of process improvement initiatives.
- Develop a business case and vision for major improvements and make sure secondary improvements align with vision and strategy.

Process Improvement Considerations

- Create architecture for process improvement to facilitate the formation of improvement teams when needed. Identify key initiatives and leaders (generally process owners and key users). Understand and facilitate required modifications in organizational structure and responsibilities.
- Build and facilitate comprehensive communications strategies, ensuring that project expectations are confirmed, understood, and periodically reconfirmed by the executive sponsors, implementation team, process owners, and users.
- Establish performance measures and monitor results.
- Build knowledge, skills, and capabilities within the workforce through training, performance support tools, and knowledge transfer. This is critical to ensuring that the process improvement philosophy (i.e., culture) is institutionalized and the process becomes self-sustaining and employee initiated.

Process improvement complements Act compliance because it not only ensures that businesses capitalize on the knowledge obtained, but also creates the opportunity to realize a return on investment from compliance initiatives. The ultimate rationale for continuous business process improvement is that it is a catalyst for making good businesses great. Keep process improvement broad, visible, simple, focused, and flexible. Try to restrain from the mentality of instant fixes and instead maintain a relentless focus toward the achievement of continuous process improvement.

Great companies are relentless in their drive to not settle for good, but to be great in everything they do. Use Act compliance as the catalyst for process improvement and transcend “the curse of competence.”⁶

NOTES

1. Results of Survey of Sarbanes-Oxley Section 404 Project Leaders at Major Companies, PricewaterhouseCoopers, page 3, January 2004.
Finding: Over half the respondents reported that the predominant perception of senior executives and the board is that Sarbanes-Oxley compliance is a necessary cost of doing business, while over 40% reported the perception that Sarbanes-Oxley will ultimately make them more competitive.

Beyond Compliance

2. *Id.*
3. Jim Collins, *Good to Great: Why Some Companies Make the Leap . . . And Others Don't*, HarperCollins Publishers, 2001, page 100.
4. *Id.*
5. These five points were derived from Robert W. Halls' *Attaining Manufacturing Excellence*, McGraw-Hill Publishing, 1986, pages 27–31.
6. *Id.*

INTERNATIONAL FINANCIAL REPORTING STANDARDS

The Sarbanes-Oxley Act of 2002 was a specific response to improve the accuracy and transparency of financial reports and corporate disclosures in the United States, yet the implications of the legislation have had a global reach. In July 2002, the European Commission announced that publicly traded companies are required to apply a single set of international accounting standards for the preparation of their consolidated financial statements. The introduction of International Financial Reporting Standards (IFRS) is intended to give investors and other stakeholders access to high-quality financial information that, for the first time, can be compared across international borders. IFRS is a comprehensive set of accounting principles defined by the International Accounting Standards Board and will be released in final form on March 31, 2005.

IFRS has been perceived to be the one of the biggest things to happen to accounting for 150 years, affecting over 7,000 companies listed on a European stock exchange. It is likely that U.S. operations of European Union (EU) companies will be required to prepare accounts according to IFRS.

All EU-listed companies are required to prepare their financial statements based on IFRS for periods beginning on or after January 1, 2005. For companies with a December 31 year end, the first full set of IFRS-compliant statements may not be published until the first quarter (Q1) of 2006; however, companies are required to produce interim results using the accounting policies that will be used in the subsequent annual financial statement. Therefore, any company producing interim results in Q1 2005 should do so according to IFRS.

The Committee of European Securities Regulators (CESR) surprised companies when it requested that a comparison of IFRS transition progress

Beyond Compliance

and key accounting differences between IFRS and generally accepted accounting principles (GAAP) be included as early as the 2003 financial statements. Analysts and investors are also starting to call for more information on IFRS. Some investment analysts have reported that IFRS readiness will be included in their evaluation of management performance, which implies that the inability to demonstrate IFRS preparedness for 2005 may be damaging to stakeholders.

COMMUNICATING THE IMPACT

The CESR has issued proposals on how EU publicly traded companies should effectively communicate the impact of the change from GAAP to international accounting standards (IAS). CESR proposes that listed companies should:

- Communicate in their 2003 financial statements how they intend to carry out the transition to international standards and explain the key differences in the accounting methods that have been identified
- Quantify in their 2004 statements the impact of the new standards on their 2004 financial statements
- Consider which accounting rules should be adopted in their quarterly and half-year financial data that will be released in 2005
- Restate comparative information for previous interim reporting periods according to IFRS
- Use a format for presenting the financial information that facilitates the understanding of the differences between accounts drawn up under previous accounting standards and those under IFRS

In addition, IFRS will have a significant impact on a number of specific accounting issues such as financial instruments, derivatives, business combinations, and foreign exchange. IFRS-related accounting issues impacting a business will be a major determinant in assessing the technical complexity, financial/business impact, and difficulty in implementing IFRS requirements.

When evaluating the specific accounting issues along with the technical recommendations, one must conclude that IFRS compliance is more than just another finance project. It is a multifaceted requirement that encom-

International Financial Reporting Standards

passes various issues relating to accounting and reporting, systems and processes, people, and the business as a whole. These issues go well beyond the mere technical issues of applying the IFRS to accounting and reporting.

THE ACCOUNTING ISSUE

Naturally, the advent of IFRS is an accounting issue. With the issuance of a set of 15 revised standards by the International Accounting Standards Board (IASB) in mid-December 2003, the current set of IAS to which companies will have to comply is already becoming well known. In addition, there will be several accounting changes from U.K. GAAP, including the methods of accounting for goodwill, business combinations, and intangible assets to name a few. Reporting of financial statement information will also change.

It is not just the accounting itself that will change. The presentation and reporting of financial results will also be affected (e.g., segmental reporting and reclassification of certain equity items as debt). Furthermore, decisions will need to be made on how to effectively introduce these changes.

THE SYSTEMS AND PROCESSES ISSUES

The changes in accounting and the approach adopted will have, in some instances, a significant impact on information technology (IT) systems. Companies will need to determine early in the process if their existing legacy systems have the capability of dealing with the financial reporting requirements of IFRS. Depending on the transition approach adopted, an organization may require a financial system that can handle both GAAP and IFRS. This is especially true of companies that need to report in both the EU and the United States. The allocation of sales, profit, and assets to a company's primary segment disclosure is likely to mean changes in data capture requirements. Currently, the readiness of software vendors to offer solutions that embrace IFRS varies, but that does not relieve the business of its responsibility to comply with the standards. Standards like compliance with Sarbanes-Oxley will also drive changes to processes and internal controls. Unfortunately, a business may be at risk for manual workarounds if its systems cannot effectively deal with the IFRS requirements.

THE BUSINESS ISSUE

The transition to IFRS affects both internal and external stakeholders and has fundamental implications for all complying companies. The following are some examples of the implications:

- Accounting changes will alter reported profits, which may require a complete review of a company's remuneration structure to the extent that the organization's compensation schemes are related to profit.
- Changes in reported profit will affect equity and reserves, which may require a revisit of the company's dividend policy.
- The reclassification of some forms of equity as debt may cause debt covenants to be breached and may require renegotiation of loans.
- Segmental reporting may disclose more information in the financial statements than previously reported and companies will need to be prepared to explain such information to investors and analysts.
- Key performance metrics may change in value under new accounting rules, and therefore may need to be evaluated to determine whether they are still relevant and an accurate measure of the underlying business.
- An organization must continue to effectively manage the business during the transition while continuing to understand and implement the requirements.

These implications do not even address the potential volatility that may be caused by accounting for financial instruments under International Accounting Standard 39, Financial Instruments: Recognition and Measurement.

THE PEOPLE ISSUE

Like most significant change initiatives, the success of the business's IFRS transition will be heavily dependent on the employees of the business. First, the initiative must have strong and visible sponsorship from executive management. If the proper tone is set from the start by executive management, employees will be more motivated and likely to support the change. Do not ignore cultural and language barriers. Often there are subtle issues that are

International Financial Reporting Standards

missed during communication because of differences in language or culture. These issues can cause problems and an organization should strive to ensure communication is clearly understood by all. Recognize that IFRS initiatives are going to require a significant investment in employee resources. It is critical that resource needs be identified early in the process to ensure that skilled employees are available at the appropriate time.

For all of the reasons listed above, the implementation of IFRS must be board sponsored and involve all areas of the organization. Set the tone at the top, set it early, and involve all applicable functional areas.

PREPARING FOR INTERNATIONAL FINANCIAL REPORTING STANDARDS

Some companies delayed getting ready for IFRS while they waited for the final text of the standards and found themselves needing to make rapid progress in IFRS implementation while the European Commission arranged for the final standards to be endorsed. These companies must now move rapidly ahead with their plans and make swift progress while also managing other large corporate changes such as Sarbanes-Oxley and Basel II requirements.

An organization must make the decision as whether to adopt an “IFRS-light” approach, which would require only implementing the bare minimum required for compliance, or seek to maximize the value from the investment required to improve the overall effectiveness of the finance function.

It is likely that there will be additional IFRS standards published. Therefore, it may be worthwhile to take an approach that goes beyond mere compliance to examine current processes and systems. Exhibit 10.1 outlines a comprehensive approach for transitioning to the new accounting

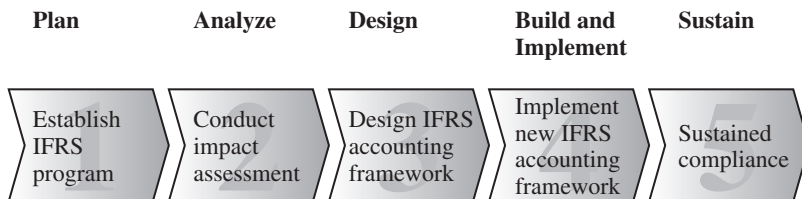


Exhibit 10.1 Comprehensive IFRS Transition Approach

standards that improves data transparency and comparability through process improvements.

Step 1. Establish the IFRS Program (Plan)

The objectives in Step 1 are to initiate the project, mobilize a senior management team, and, most importantly, understand IFRS requirements. Many similar project plans begin with an assessment of the impact of IFRS on the company without serious consideration being given to IFRS itself. The comprehensive approach displayed in Exhibit 10.1 dedicates a separate step for understanding IFRS, its background, and its relationship to other IASB projects, especially GAAP convergence. This will provide a much better basis on which to proceed to Step 2 (analyze). During Step 1, the governance for the project (including the formation of a steering committee drawn from across the business) is established and an initial project plan is prepared and approved. The plan delineates key activities, milestones, and resources. Key Step 1 activities include:

- Establish a program director and core team.
- Form a corporate governance steering committee.
- Compare and understand IFRS, country-specific accounting requirements, U.S. GAAP, and Sarbanes-Oxley requirements.
- Align IFRS efforts with current initiatives.
- Define project scope.
- Mobilize executive management as the program champions.

Step 2. Assess the Impact of IFRS (Analyze)

While a main principle of any set of accounting standards is to promote transparency, comparability, and consistency in accounting treatment, the migration to the current set of revised international accounting standards does allow for some choice. In particular, it might be argued that with IFRS, the IASB has opted to sacrifice a degree of comparability in an effort to reduce the costs of transition. During Step 2, therefore, it is essential to determine what options are available during transition and what treatments will not survive the transition year. Using scenarios will be very useful at this point.

International Financial Reporting Standards

At the end of Step 2, the company should have a clear idea of the impact of IFRS and be able to determine the implications for internal control, policy, process, and IT system changes. A communication plan can then be developed to inform internal and external stakeholders. Key aspects of Step 2 include:

- Determining the effect of IFRS on key metrics
- Understanding and communicating implications for budgeting, strategic plans, and investor expectations
- Consideration of behavioral aspects
- Results simulations and “what if” analysis
- IT system requirements
- Change Management implications (see Chapter 5)
- Project scope refinement

Step 3. Create the New IFRS Accounting Framework (Design)

The detailed preparation begins during this step. Cross-functional design teams are assigned the task of developing the practical means for the transition to IFRS and identifying the implications beyond the transition year. The proposed solutions will be tested and final sign-off of an agreed-upon solution will be secured. The exact project structure, number of design teams, and work to be conducted during this phase will depend on the results of Step 2.

At the end of this step, a company will have a detailed migration plan, revised project plan, and resource budget, and will have commenced the communications program. During Step 3, training needs and materials will also have been identified and developed. Key aspects of Step 3 include:

- Define new policies, procedures, practices, and processes.
- Develop a new chart of accounts.
- Configure IT systems.
- Plan and execute potential restatements.
- Establish data migration parameters.
- Produce training materials and employee training schedule.
- Finalize the “cutover” strategy.

Step 4. Execute the New IFRS Accounting Framework (Build and Implement)

Step 4 is where the design is implemented. Design teams transition to implementation teams, and a pilot and/or parallel run is conducted to ensure that expected results are achieved. The communications program is executed and investors as well as analysts are made aware of the implications of an effective implementation on the company's financial reporting. During this step, it is also essential to determine how the further implementation of IFRS will be sustained beyond the transition year since there will be further change to incorporate in year 2. Key aspects of Step 4 include:

- Roll out new systems, test, reconcile, and run parallel (as appropriate).
- Conduct training.
- Create support/help desk.
- Cut over to new systems.
- Stabilize new systems, controls, and processes.
- Create new reporting organizations.

Step 5. Continue Compliance (Sustain)

During this final step, companies should embed IFRS in subsidiaries, if not already completed, and continue to monitor the relevance and link between management information and IFRS. Scenario analysis should also be continued as new or revised standards are published.

Underpinning each step will be the need for strong program management to ensure that milestones are being adhered to, risks identified and managed, and costs of implementation controlled. The benefits of introducing other changes to support IFRS (e.g., management reporting) should also be tracked to ensure that they are being achieved.

The transition to IFRS should be undertaken as a major change event within an organization and should secure board sponsorship and the utilization of cross-functional project teams. Treating the change effort as a finance-only project will severely compromise a successful implementation. Key aspects of Step 5 include:

- Transition steering committee responsibility to ongoing compliance.
- Ensure the steering committee is aware of new IFRS requirements.

- Embed IFRS in subsidiaries.
- Continue to monitor the relevance and linkage between management information and IFRS.

KEY ELEMENTS OF AN EFFECTIVE IFRS IMPLEMENTATION

The preceding five steps outline a comprehensive approach to IFRS transition and compliance. To get the most out of this approach, additional issues should be analyzed and considered. The five-step approach and the following issues should be considered based on the business-specific circumstances and modified as appropriate.

Ensure Board-Level Buy In

At a minimum, financial managers must secure the support of the chief executive officer (CEO), chief operating officer (COO), chief information officer (CIO), audit committee, and operating controller. This step is probably the most critical for ensuring a successful implementation; therefore, financial managers must make it their responsibility to champion change, justifying their proposition to these individuals to ensure their support.

Set Up an IFRS Transition Team

While team requirements and structure will vary among companies, there are certain key roles that must be filled on each project. Financial managers should recruit people for several positions:

- *Steering committee.* This group should have representation from all interested parties, from relevant board members such as the CEO, COO, and CIO through representatives from finance and IT.
- *Project manager.* Appointed by the steering committee, this person will be responsible for managing the project on a day-to-day basis; addressing the risks and issues; and achieving the project's objectives related to time, budget, and quality.
- *Change and communications manager.* This critical position focuses on the people, internal or external, who are affected by the change to

Beyond Compliance

ensure their commitment is obtained and the project realizes its full benefits. An IFRS implementation project will involve changes to a company's IT systems, financial processes, and internal and external communications, and may require the development of new roles and responsibilities and the acquisition of new skills by end users.

- *Technical accounting and policy lead.* This person is responsible for understanding the company's IFRS requirements; identifying what additional data is required to fulfill these requirements; communicating these requirements to the process reengineering lead; understanding the nature of any material changes to the financial statements; and identifying where changes need to be made to the current IT systems and communicating those changes to the IT lead.
- *Process reengineering lead.* This position focuses on implementing necessary change. The individual that fills this role must determine the source of additional data; redesign the processes to ensure the additional data is captured; assess the impact of these changes on the close process; work closely with the technical accounting and IT leads to prepare systems requirements; and test the redesigned systems and processes.
- *IT lead.* This individual will take the systems requirements and redesign and test the IT infrastructure, as necessary.
- *Training lead.* This person must work with each lead to identify training requirements and therefore should be finance and IT savvy. Responsibilities include developing and conducting the training with the required user groups.

Agree Upon Deliverables

Once the project team is in place, financial managers should agree on the deliverables to ensure the project objectives are met. Specific tasks to complete at this point in the effort include:

- Setting the project objective
- Introducing team members and their project roles
- Highlighting the timetable
- Clarifying the internal reporting and communication requirements

Step Away from the Detail

Financial managers should trust the team to deliver the objectives and allow the project manager and other team leads to work toward achieving key milestones. Financial managers should stay abreast of any significant changes to financial statements and communicate those changes in a timely manner to stakeholders. In the final analysis, IFRS implementation is much more than a finance issue. It requires input and active involvement of employees from virtually all levels of the business from the board to process owners and from the corporate office to each operating location. Combining the five-step approach with the appropriate level of employee involvement will go a long way toward ensuring a successful IFRS implementation initiative.

NON-U.S.-BASED COMPANIES AND SARBANES-OXLEY COMPLIANCE

Compliance with the provisions of the Sarbanes-Oxley Act of 2002 is an issue not just for U.S. publicly traded companies. It is a significant piece of legislation that reaches outside the borders of the United States to affect many foreign corporations. Non-U.S.-based companies need to review the Act and related Securities and Exchange Commission (SEC) and Public Company Accounting Oversight Board rules and pronouncements and determine how the Act applies to their business. The extensive requirements of Act compliance and the resultant commitment of effort and time warrant non-U.S.-based companies to promptly address their Act compliance requirements.

WHO IS AFFECTED BY SARBANES-OXLEY?

(Note: The following paragraphs are meant to provide a summary understanding of the Act for non-U.S.-based companies. Refer to Chapters 1 through 4 for guidance on the detailed financial compliance provisions of the Act, specifically Sections 302 and 404.)

The Sarbanes-Oxley Act of 2002 was signed into law to improve the accuracy and transparency of financial reports and corporate disclosures, as well as to reinforce the importance of corporate ethical standards. The provisions of the Act apply to all SEC-registered companies, including those with either debt or equity listings. *Non-U.S.-based companies affected consist of foreign subsidiaries of U.S. companies as well as companies dually listed on both a non-U.S. and U.S. stock exchange.*

Beyond Compliance

There are three key features of the Act that require compliance and relate to the financial reporting process for foreign subsidiaries of U.S. companies as well as dually listed non-U.S.-based companies (hereafter referred to as “affected companies”):

- *Section 302.* Requires management to certify the quarterly and annual financial statements and management’s assessment of disclosure controls and internal controls for financial reporting.
- *Section 404.* Requires all annual reports to include the results of management’s assessment of their internal controls over financial reporting and an independent verification of the accuracy of management’s assessment, as well as an attestation, from the company’s external auditor.
- *Section 409.* Requires companies to make real-time disclosures of information concerning material changes in the financial condition or operations of the company.

Affected companies were required to comply with Section 302 provisions for all filings submitted on or after August 29, 2002, and the provisions of Section 409 as prescribed by the revised SEC Form 8-K disclosure requirements.¹ Finally, foreign subsidiaries of U.S.-based corporations and non-U.S.-based corporations with U.S. dual listings (i.e., SEC-registered non-U.S.-based companies) must comply with the provisions of Section 404 for fiscal years ending on or after June, 2006.

Affected companies should follow an Act compliance approach similar to the approaches detailed in Chapter 4 in order to achieve compliance and facilitate an auditor attestation of management’s assessment of internal control over financial reporting. Any approach to Act compliance should include close interaction with the business’s external auditor in validating the in-scope processes and locations and the documentation methodology.

WHO SHOULD HAVE THIS ON THEIR AGENDA?

While the chief executive officer (CEO) and chief financial officer (CFO) have ultimate responsibility for the Section 302 and Section 404 certifications, Act compliance initiatives, or at least the initial approach, should be designed and implemented by a dedicated team and actively supported by

Non-U.S.-Based Companies and Sarbanes-Oxley Compliance

senior management. This team should report to a steering committee consisting of executive management. The importance of effective internal control must be understood as part of the process in all business functions (e.g., purchase to pay, order to cash) and ingrained in the culture of the entire organization.

WHAT PREPARATION IS REQUIRED TO ENSURE COMPLIANCE?

Compliance with the Act is not a small undertaking and should not be looked upon lightly. Depending on the size of an organization, compliance will take months to achieve. Nevertheless, a company's efforts can be greatly rewarded. A well-implemented Act compliance initiative can achieve a return on investment well beyond mere compliance. The following compliance approach overview should provide some understanding of the scale of the work involved (see Chapter 4 for a detailed approach to Act compliance).

Build a Compelling Business Case

Develop a vision for your organization that is based on a platform of internal controls. Build a business case to support this vision. In doing this, consider the following:

- Most public companies already have some form of internal controls in place. Existing systems, processes, and resources should be leveraged when developing a more formalized approach. Improved processes and systems will result in more accurate and timely information, which will enable better business decision making. Additional benefits could also include cost reduction opportunities through process and system efficiencies.
- Strong corporate governance enhances shareholder value regardless of whether the company is public or private. One study indicated that a company with strong governance could command as much as an 18% premium on its market value.²
- Given that governance extends beyond the finance and accounting departments, the implementation of a regular training program will promote and maintain enterprise-wide awareness.

Beyond Compliance

- An adequate investment in the first year of compliance will form a sound basis for the compliance efforts in subsequent years and can give management assurance over the quality of certifications for years to come.

Establish an Internal Control Framework

The Sarbanes-Oxley legislation recognizes the Committee of Sponsoring Organizations (COSO) Treadway commission and the U.K.-originated Turnbull Report as providing suitable models for the establishment of effective internal controls. The Turnbull Report, published by the Institute of Chartered Accountants in England and Wales, will already be familiar to U.K. organizations in providing guidance as to how to adopt a risk-based approach to establishing an effective internal control system. Either of these frameworks to compliance is acceptable for affected companies.

Assess the Existing Internal Control Environment

Evaluate Effectiveness of Existing Controls

Obtain an in-depth understanding of the current internal control environment to help determine the level of effort required to achieve Act compliance. Determine whether policies, procedures, and controls are:

- Appropriately documented
- Standardized throughout the organization
- Communicated effectively
- Applied consistently

Also, establish whether there is a process in place to monitor compliance. Performing such a self-assessment can be an important first step in developing an Act compliance plan and setting priorities.

Identify High-Risk/Reward Areas

Identify financial reporting and disclosure risks that could adversely affect your company's ability to accurately report financial and non-financial data. High-risk areas can be identified through the completion of control self-assessment documentation or from the results of previously published

Non-U.S.-Based Companies and Sarbanes-Oxley Compliance

internal audit reports or management letters, as well as through management input and internal and external auditors. Document and prioritize these risks based on factors such as inherent business risks to the company, materiality to the financial statements, and likelihood of occurrence.

Determine Appropriate Level of Control

Review the identified financial reporting and disclosure risks and define key control objectives to address each one.

Compare Current State to Target Levels

Review the control process in each high-risk/reward area through a series of interviews and observations. Compare the existing controls and procedures against the target control objectives. Identify control gaps in existing processes, assess the potential impact, and document remediation/improvement options.

Implement Remediation/Improvements Options

Communicate and Train

The business needs to understand the importance of embracing a strong internal control culture. Establishing responsibilities and conveying information to employees in a format and time frame that allows them to effectively perform their internal control responsibilities is a requisite.

Ensure that Documentation Can Pass Scrutiny of Third-Party Review

The new internal control processes should be evident throughout the organization. Written policies and processes are a minimum requirement. Evidence of review and authorizations, reconciliations, and external verification is needed. Implementing a system of internal controls is not a one-time effort but an ongoing absolute for Act compliance.

Responsibility for Monitoring

Disclosure and Communication

Section 302 of the Act recommends the formation of a disclosure committee. Typically this would be chaired by the CFO and be made up of key business leaders, including the chief operating officer. This committee

Beyond Compliance

should serve as an information conduit to the audit committee in determining disclosable events such as deficiencies in internal control and instances of management fraud. A formal reporting and monitoring process, along with encouraging employees to communicate results, issues, or deficiencies in internal controls to management, is vital to ensuring timely and accurate reporting.

Establish a Process for Continuous Improvement

In an optimized environment, change efforts can be undertaken in real time. Continual reviews will ensure that processes are not stagnant, while retaining the company's ability to respond quickly to industry, market, and technology changes.

Certify with Confidence and Avoid Prosecution

Once Act compliance initiatives have been implemented, executives will be able to certify with confidence knowing their company's internal standards exceed those dictated by any regulatory body.

Noncompliance will severely impact shareholder confidence. An incorrect certification by management can result in stiff penalties being imposed (including imprisonment of the CEO/CFO), in addition to damaging shareholder confidence and a company's corporate reputation.

Some have described Sarbanes-Oxley as the most significant piece of business legislation since the Securities Acts of the 1930s. Whether you agree with that observation or not, the Act has unmistakably changed the business and regulatory environment and companies cannot afford to underestimate its impact. Regardless of the current operational infrastructure, being able to demonstrate a strong system of internal control can lead to competitive advantages that produce tangible results.

NOTES

1. SEC Release No. 33-8400. Additional Form 8-K Disclosure Requirements and Acceleration of Filing Date, March 16, 2004.
2. "Three surveys on corporate governance," Paul Coombes and Mark Watson, *McKinsey Quarterly*, November 4, 2000.

FINANCIAL SERVICES COMPLIANCE INITIATIVES

As a result of passage of the Sarbanes-Oxley Act, many other countries and jurisdictions have begun to investigate, debate, and adopt similar legislation. For example, in the European Union (EU), the International Accounting Standards Board on March 31, 2004, released a comprehensive set of accounting standards, the International Financial Reporting Standards (IFRS), intended to give investors and other stakeholders access to high-quality financial information that, for the first time, can be compared across international borders (see Chapter 10).

As a result, the first decade of the 21st century will be recalled as a period of sweeping business reform as a consequence of the focus on increasing regulation, a general strengthening of the governance framework, and an invigorated and intense focus on internal control over financial reporting and disclosure. Even organizations that are not initially directly affected by the changes are considering the impact and adopting best practice approaches around governance and compliance. Although derived from different sources and backgrounds, and developed for different reasons, these changes are inextricably linked to one another, particularly for global financial services companies that are impacted by all the changes.

The legal and regulatory frameworks surrounding governance are continuously becoming more complex and interwoven. There is an ever-increasing range of measures and benchmarks emerging in different regions around the globe. In the United Kingdom, for example, governance requirements and guidelines were consolidated in the 2003 revised Combined Code on Corporate Governance annexed to the U.K. Listing Rules by the Financial Services Authority.¹ For many U.K. companies that

have dual exchange listings or debt listing overseas, rules applied in the country of listing will also need to be addressed and complied with. As discussed in Chapter 11, the Sarbanes-Oxley Act is applicable to all U.K. companies with a U.S. listing, and therefore, such companies will need to comply with both sets of regulations.

This chapter examines some of the features of the changing corporate governance and compliance environment, including regulatory changes, and their relationship to the financial services companies. These changes impact not only all the external corporate sectors that they service but also affect the industry's own governance and compliance. The major governance and compliance initiatives facing financial services organizations are Sarbanes-Oxley, International Financial Reporting Standards, Basel II, and Solvency II.

SARBANES-OXLEY AND EQUIVALENT LEGISLATION

The Sarbanes-Oxley Act of 2002 materially changed the risks and responsibilities for directors and officers of public companies. Under the Act, chief executive officers (CEOs) and chief financial officers are required to certify and are personally liable for the accuracy of certain parts of the business's financial reports. In addition, they must certify that sound internal control processes are in place and have been assessed by management. These regulations make the obligations and actions of directors and officers specific and transparent. Claims against directors and officers arising from nonperformance will be similarly focused.

The Act has had a global reach. Many international companies that are not U.S. based but have a U.S. share or debt listing must comply with the Act. In addition, many U.S. companies that are not listed are beginning to adopt full Act compliance as a business best practice. These organizations believe that their profile requires confidence in their controls and procedures and the adoption of best practices that are in line with their publicly traded peers is a potential competitive advantage.

Other countries are beginning to introduce similar legislation. The Canadian Securities Administrators rules 52-108, -109, and -110, broadly based around the Act, but tailored to the Canadian markets, became effective in 2004. In Ireland, the Companies Auditing & Accounting Bill 2003 (IAASA Bill) was enacted. The directors' compliance statement required under the IAASA Bill covers compliance with the Companies Acts, tax law, and other "relevant" law that could affect materially the company's

financial statements. According to the Institute of Chartered Accountants in Ireland “no other country in the developed world requires directors to sign a statement such as this.” The Bill also establishes the role of the audit committee in law, requiring even private companies over a certain size to explain if they do not have such a committee, another example of compliance extending beyond the public company listings.

This provides specific business risk for insurers who must be aware of the broadening implications that this may have on the directors’ and officers’ coverage they are providing and how they assess risks and advise their clients on mitigation. Equally, they must also monitor their own compliance with this type of regulation.

International Financial Reporting Standards

The International Accounting Standards Board (IASB), comprised of members from nine countries, is charged with delivering high-quality, understandable, and enforceable global accounting standards: the International Financial Reporting Standards (IFRS). Its predecessor until 2001, the International Accounting Standards Committee, issued more than 40 standards that have been adopted within the IFRS framework but will continue to be designated as international accounting standards (IAS). The IASB and U.S. Financial Accounting Standards Board are working on convergence of IFRS with U.S. generally accepted accounting principles (GAAP).

All EU-listed companies are required to prepare their financial statements in line with IFRS from 2005 (including 2004 comparatives). Differences between IFRS and U.S. GAAP will, however, persist well beyond that date.

The financial services sector, particularly the insurance sector, has had to overcome significant issues surrounding valuations brought about by IAS 39 Financial Instruments: Disclosure and Measurement. The move to fair value pricing of financial assets and liabilities may create accounting volatility as well as some regulatory inconsistencies that still have to be resolved.

The IASB has just issued IFRS 4, aimed at improving disclosures for insurance contracts and some improvement in recognition and measurement practices in preparation for the starting date of 2005. A second phase of the IASB’s accounting project is just commencing to address broader conceptual and practical issues related to insurance accounting. This phase, which will eventually introduce fair value for an insurance company’s

Beyond Compliance

liabilities, may take several years to complete, and, in Europe, will have to integrate with the requirements of Solvency II. However, the IASB has indicated its willingness to revise IFRS 4 in the short term for any immediate solutions identified.

As the new accounting standards become effective in each country, the directors and officers are responsible for application of the new rules and their disclosure in the published accounts. In addition, the revised reporting, analysis, and valuation treatments contained within the rules directly impact the topics discussed below, and consequently their successful integration and application in Sarbanes-Oxley, Basel II, or Solvency II programs is crucial.

Basel II

The first Basel Capital Accord (named after the Basel Committee of the Bank for International Settlements) was introduced in 1988. This set out a credit risk measurement framework along with a minimum capital standard of 8%. Progressively deployed in virtually every country with active international banks, the first Accord is about to be replaced by the new Accord, Basel II, as of 2007.

Basel II will be applied to all banks, investment firms, and similar organizations. The rules are intended to promote sound supervisory standards, provide a robust capital adequacy framework, and encourage international convergence toward common approaches and standards. This is achieved through three pillars:

Pillar 1: Minimum capital requirements. This sets out a new framework for calculating capital requirements based on better calibration and a more risk-sensitive approach by refining the standardized rules of the first accord and adding a capital requirement for operational risk.

Pillar 2: Supervisory review of capital adequacy and internal assessment processes. Compliance with Basel II will involve not just the calculation of capital under a new set of rules but the whole framework of management, governance, systems, and processes of the entire organization. There is considerable overlap with the internal control framework of Turnbull, and for firms with a U.S. listing,

Financial Services Compliance Initiatives

with the Sarbanes-Oxley internal control assessments and certification. This is where firms may struggle to undertake the changes to systems and procedures needed to satisfy the regulators' expectations.

Pillar 3: Market discipline through effective disclosure that encourages safe and sound insurance practices. The impact of the new international accounting standards must be taken into account where analysis and disclosure will need to reflect the new rules to strengthen market discipline as a complement to the supervisory effort.

In the United States, only the top 10 banks are currently required to adopt Basel II, but in so doing will adopt the most advanced credit and operational risk methodologies available. The next 10 will also follow, but there are no plans to require smaller banks to adopt Basel II. Financial growth, peer pressure, and public perception are all likely to encourage wider adoption of the new standards over time.

Interestingly, exempt from Basel II are the U.S. investment banks, not currently covered by the rules (although overseas subsidiaries will have to comply with local Basel II requirements). However, pressure from the EU for a level playing field is likely to remove this exemption.

Who is interested in the level of compliance with Basel II apart from the regulators? Investors as well as other stakeholders including rating agencies, counterparty banks, plus the media and consumer groups are interested in compliance. Insurers will also take a close interest in the situation. Overall, Basel II is about better risk management and better governance on a continuous basis. Insurers must understand the complex relationships that the new culture is creating, and consider carefully how their approach to risk management must become proactive in understanding and advising their clients. Market confidence and shareholder value are all too easily dented by any perceived weaknesses.

Solvency II

Solvency II will create for European insurance companies a capital and risk management framework that corresponds with the Basel II framework for banks. The European Solvency Directives aim to provide consistent policyholder protection and a level playing field between undertakings across the

EU. The solvency margin provides a buffer of capital against unforeseen events.

The first Solvency Directive, in 2002, strengthened and improved on existing rules dating back to the 1970s. The plans for Solvency II are much broader in scope, covering developments in insurance, risk management, finance techniques, and financial reporting. Solvency II adopts the three-pillar approach of Basel II, but much work has yet to be done before a full draft directive is presented. This is not expected before the end of 2005, with final implementation expected to take two to five additional years.

In the United Kingdom, the Financial Services Authority (FSA) is accelerating the implementation of many aspects of Solvency II, introducing best practices in compliance, management, supervision, and controls across all sectors of financial services as part of a rigorous supervisory regime. Currently incorporated in the FSA's Prudential Sourcebook, this framework will adapt to the future requirements of Solvency II as they become part of EU and U.K. law.

The insurance industry will have to get used to a level of regulatory scrutiny of internal controls and procedures that the banking community has been well exposed to for many years. For example, Section 39 of the 1987 Banking Act included a provision whereby the regulator could require a bank to provide a report on any area of its activities, this review to be undertaken by a reporting accountant, generally the bank's external auditor.

In the early days, topics such as high-level controls were raised annually, covering areas very similar to the framework now seen under the Turnbull (the United Kingdom's best practices standards on internal control) combined code on internal controls. More detailed themes and scope quickly developed. Around the mid-1990s, the Bank of England extended the scope and detail of its scrutiny through the deployment of the Traded Markets Team, specializing in reviews of the systems and procedures expected in the more complex treasury and trading operations.

The old Section 39 powers continue to be maintained in the Financial Services and Markets Act 2000, with the scope now extended across the financial services sector. In addition, direct regulator scrutiny is also implemented under the Arrow Risk Assessment process. Given the substantial processes that must be already developing to meet the FSA's Prudential Sourcebook requirements and the capital calculations, a coordinated program for Solvency II is vital to set the road map for compliance. Solvency II will subject the directors and officers of insurers to the same degree of transparency and scrutiny as will be applied to banks and other

Financial Services Compliance Initiatives

financial institutions under Basel II. Processes, controls, systems, and management structures must adapt accordingly.

All four of these initiatives—Sarbanes-Oxley, IFRS, Basel II, and Solvency II—will have an effect on financial services organizations. A large number of financial services organizations will have to comply with two or more of these initiatives as well as other specific country requirements. Fortunately there is some overlap of coverage, which can be leveraged to reduce the cost of implementation and increase the effectiveness and efficiency of governance activities. Exhibit 12.1 shows that topics such as the Committee of Sponsoring Organizations (COSO) and Control Objectives for Information and Related Technology (COBIT) frameworks; treatment

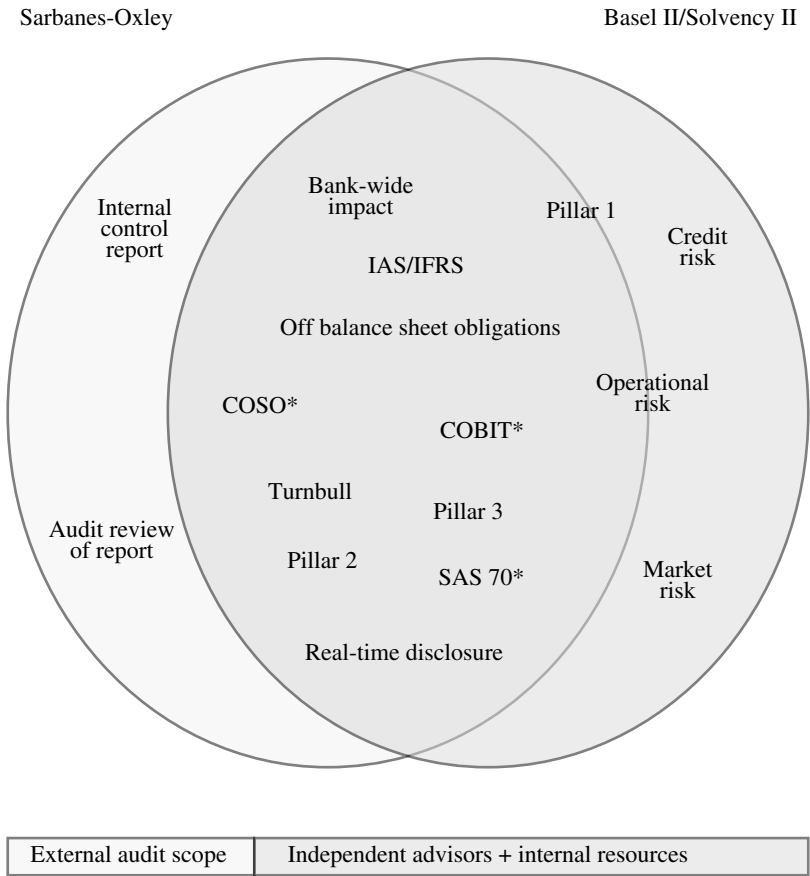


Exhibit 12.1 Examine the Areas of Overlap

Beyond Compliance

of off balance sheet obligations; Pillar 2 and Pillar 3 concepts; Statement on Accounting Standard (SAS) 70 reports; and real-time disclosures are themes that are incorporated in Sarbanes-Oxley, Basel II, and Solvency II. Financial services organizations should take advantage of this overlap in planning and designing their governance programs. An integrated approach to governance will eliminate duplicate efforts and maximize resource utilization.

EFFECTIVE COMPLIANCE TO DELIVER BUSINESS VALUE

The costs involved in meeting compliance for financial services organizations can be significant. Any international bank is charged with meeting a combination of Sarbanes-Oxley and Basel II as well as local regulatory requirements. However, the investment made to deliver compliance can actually be used as an advantage to provide better performance and increase business value. The process mapping, analysis of key controls, and gathering of loss event data all provide senior management with an up-to-date and enterprisewide view.

Mapping the organization's processes may reveal hidden opportunities for shared services, occasions to streamline processes and reduce costs. A more dynamic system of internal controls with traffic light monitoring and feedback will not only provide management with a more effective means of supervising the business but should also be used to contain audit fees through well-documented and visible processes. Financial services organizations should consider utilizing a compliance model similar to the one shown in Exhibit 12.2 to assist in the integration of their governance and compliance efforts. This model examines all of the decision support objects, coupled with the business driver (Sarbanes-Oxley, Basel II, Solvency II) requirements, as well as business strategy and goals to drive value.

For financial services organizations, the demands for and expectations of better and more transparent governance now comes from many sources. Shareholders, customers, analysts, rating agencies, the press, auditors, insurers, bankers, lobby groups, and regulators are all taking a keen interest in the governance profile of public companies.

A significant development also emerging is the number of nonpublic companies in the United States that are starting to voluntarily adopt Sarbanes-Oxley compliance programs. These include organizations that have a high public profile. Their CEOs want to be comfortable with the knowl-

Create a Finance Model for Effective Compliance

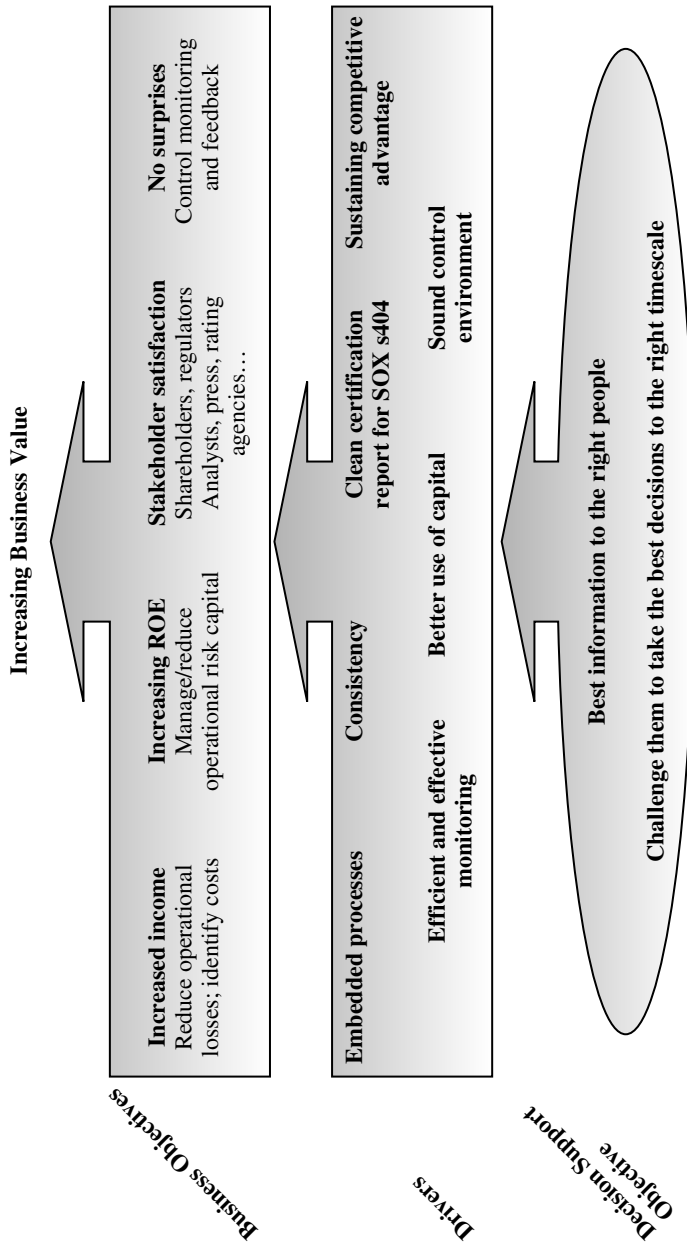


Exhibit 12.2 An Effective Compliance Model

© 2004 Parson Consulting.

Beyond Compliance

edge that the organization is adhering to best practices for any large and complex organization. Over time, this is likely to cascade down to smaller organizations that also want to be viewed by their stakeholders as well governed.

The Sarbanes-Oxley model is beginning to be adopted in other countries. Canada and Ireland are early adopters of equivalent rules. Proposals at the EU level and within the United Kingdom (published by the FSA) would extend the scope of audit review and opinions to include coverage of internal controls.

Any large organization that does not yet take seriously this change in the focus on governance will be in for a shock. Those that do are using it as a competitive advantage, both to win business and customers and to improve processes and controls.

NOTE

1. The Financial Services Authority is an independent nongovernmental body that regulates the financial services industry in the United Kingdom as authorized by the Financial Services and Markets Act of 2000.

APPENDIX A

SARBANES-OXLEY SECTION 302

SEC. 302. CORPORATE RESPONSIBILITY FOR FINANCIAL REPORTS

- (a) **REGULATIONS REQUIRED.** The Commission shall, by rule, require, for each company filing periodic reports under section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m, 78o(d)), that the principal executive officer or officers and the principal financial officer or officers, or persons performing similar functions, certify in each annual or quarterly report filed or submitted under either such section of such Act that—
- (1) the signing officer has reviewed the report;
 - (2) based on the officer's knowledge, the report does not contain any untrue statement of a material fact or omit to state a material fact necessary in order to make the statements made, in light of the circumstances under which such statements were made, not misleading;
 - (3) based on such officer's knowledge, the financial statements, and other financial information included in the report, fairly present in all material respects the financial condition and results of operations of the issuer as of, and for, the periods presented in the report;
 - (4) the signing officers—
 - (A) are responsible for establishing and maintaining internal controls;

Appendix A

- (B) have designed such internal controls to ensure that material information relating to the issuer and its consolidated subsidiaries is made known to such officers by others within those entities, particularly during the period in which the periodic reports are being prepared;
 - (C) have evaluated the effectiveness of the issuer's internal controls as of a date within 90 days prior to the report; and
 - (D) have presented in the report their conclusions about the effectiveness of their internal controls based on their evaluation as of that date;
- (5) the signing officers have disclosed to the issuer's auditors and the audit committee of the board of directors (or persons fulfilling the equivalent function)—
- (A) all significant deficiencies in the design or operation of internal controls which could adversely affect the issuer's ability to record, process, summarize, and report financial data and have identified for the issuer's auditors any material weaknesses in internal controls; and
 - (B) any fraud, whether or not material, that involves management or other employees who have a significant role in the issuer's internal controls; and
- (6) the signing officers have indicated in the report whether or not there were significant changes in internal controls or in other factors that could significantly affect internal controls subsequent to the date of their evaluation, including any corrective actions with regard to significant deficiencies and material weaknesses.
- (b) **FOREIGN REINCORPORATIONS HAVE NO EFFECT.** Nothing in this section 302 shall be interpreted or applied in any way to allow any issuer to lessen the legal force of the statement required under this section 302, by an issuer having reincorporated or having engaged in any other transaction that resulted in the transfer of the corporate domicile or offices of the issuer from inside the United States to outside of the United States.
- (c) **DEADLINE.** The rules required by subsection (a) shall be effective not later than 30 days after the date of enactment of this Act.

APPENDIX B

SARBANES-OXLEY SECTION 404

SEC. 404. MANAGEMENT ASSESSMENT OF INTERNAL CONTROLS

- (a) **RULES REQUIRED.** The Commission shall prescribe rules requiring each annual report required by section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m or 78o(d)) to contain an internal control report, which shall—
 - (1) state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and
 - (2) contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.
- (b) **INTERNAL CONTROL EVALUATION AND REPORTING.** With respect to the internal control assessment required by subsection (a), each registered public accounting firm that prepares or issues the audit report for the issuer shall attest to, and report on, the assessment made by the management of the issuer. An attestation made under this subsection shall be made in accordance with standards for attestation engagements issued or adopted by the Board. Any such attestation shall not be the subject of a separate engagement.

APPENDIX C

SARBANES-OXLEY SECTION 409

SEC. 409. REAL TIME ISSUER DISCLOSURES

Section 13 of the Securities Exchange Act of 1934 (15 U.S.C.78m), as amended by this Act, is amended by adding at the end the following:

“(l) REAL TIME ISSUER DISCLOSURES. Each issuer reporting under section 13(a) or 15(d) shall disclose to the public on a rapid and current basis such additional information concerning material changes in the financial condition or operations of the issuer, in plain English, which may include trend and qualitative information and graphic presentations, as the Commission determines, by rule, is necessary or useful for the protection of investors and in the public interest.”

APPENDIX D

EVALUATION QUESTIONS TO UNDERSTAND THE CURRENT STATE OF CONTROL PROCESSES

- Question 1. Are your accounting policies, practices, and procedures adequately documented, communicated, and understood throughout your organization?
- Question 2. Is your accounting staff sufficiently trained in generally accepted accounting principles (GAAP) and financial disclosure requirements to provide you with the information you need?
- Question 3. Is your internal control system adequate to detect and report errors or fraud?
- Question 4. Is your internal audit activity sufficiently independent to report errors or deviations from GAAP and approved procedures?
- Question 5. If your organization has multiple accounting locations, what procedures have you established to ensure all locations are consistently following company policies, practices, and financial reporting procedures?
- Question 6. Is your audit committee actively involved in the review of your financial reporting to shareholders? Do you have a process in place that facilitates an open and collaborative relationship with the audit committee?
- Question 7. Have you recently evaluated the risks facing your business?
- Question 8. Do you receive complete and timely financial information necessary to make informed management decisions?
- Question 9. Do you have key performance indicators that highlight issues that require attention?

APPENDIX E

INTERNAL CONTROL OVER FINANCIAL REPORTING¹

A process designed by, or under the supervision of, the company's principal executive and principal financial officers, or persons performing similar functions, and effected by the company's board of directors, management, and other personnel, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles and includes those policies and procedures that:

1. Pertain to the maintenance of records that, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the company;
2. Provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the company are being made only in accordance with authorizations of management and directors of the company; and
3. Provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the company's assets that could have a material effect on the financial statements.

¹Auditing Standard No. 2—An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements, Paragraph 7, effective pursuant to SEC Release No. 34-49884; File No. PCAOB-2004-03, June 17, 2004.

APPENDIX F

EVALUATING CONTROL DEFICIENCIES¹

130. *Evaluating deficiencies in internal control over financial reporting.* The auditor must evaluate identified control deficiencies and determine whether the deficiencies, individually or in combination, are significant deficiencies or material weaknesses. The evaluation of the significance of a deficiency should include both quantitative and qualitative factors.
131. The auditor should evaluate the significance of a deficiency in internal control over financial reporting initially by determining the following:
- The likelihood that a deficiency, or a combination of deficiencies, could result in a misstatement of an account balance or disclosure; and
 - The magnitude of the potential misstatement resulting from the deficiency or deficiencies.
132. The significance of a deficiency in internal control over financial reporting depends on the *potential* for a misstatement, not on whether a misstatement actually has occurred.
133. Several factors affect the *likelihood* that a deficiency, or a combination of deficiencies, could result in a misstatement of an account

¹Auditing Standard No. 2. An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements, Paragraphs 130–137, effective pursuant to SEC Release No. 34-49884; File No. PCAOB-2004-03, June 17, 2004.

Appendix F

balance or disclosure. The factors include, but are not limited to, the following:

- The nature of the financial statement accounts, disclosures, and assertions involved; for example, suspense accounts and related party transactions involve greater risk.
 - The susceptibility of the related assets or liability to loss or fraud; that is, greater susceptibility increases risk.
 - The subjectivity, complexity, or extent of judgment required to determine the amount involved; that is, greater subjectivity, complexity, or judgment, like that related to an accounting estimate, increases risk.
 - The cause and frequency of known or detected exceptions for the operating effectiveness of a control; for example, a control with an observed non-negligible deviation rate is a deficiency.
 - The interaction or relationship of the control with other controls; that is, the interdependence or redundancy of the control.
 - The interaction of the deficiencies; for example, when evaluating a combination of two or more deficiencies, whether the deficiencies could affect the same financial statement accounts and assertions.
 - The possible future consequences of the deficiency.
134. When evaluating the likelihood that a deficiency or combination of deficiencies could result in a misstatement, the auditor should evaluate how the controls interact with other controls. There are controls, such as information technology general controls, on which other controls depend. Some controls function together as a group of controls. Other controls overlap, in the sense that these other controls achieve the same objective.
135. Several factors affect the magnitude of the misstatement that could result from a deficiency or deficiencies in controls. The factors include, but are not limited to, the following:
- The financial statement amounts or total of transactions exposed to the deficiency.
 - The volume of activity in the account balance or class of transactions exposed to the deficiency that has occurred in the current period or that is expected in future periods.

Evaluating Control Deficiencies

136. In evaluating the magnitude of the potential misstatement, the auditor should recognize that the maximum amount that an account balance or total of transactions can be overstated is generally the recorded amount. However, the recorded amount is not a limitation on the amount of potential understatement. The auditor also should recognize that the risk of misstatement might be different for the maximum possible misstatement than for lesser possible amounts.
137. When evaluating the significance of a deficiency in internal control over financial reporting, the auditor also should determine the level of detail and degree of assurance that would satisfy prudent officials in the conduct of their own affairs that they have reasonable assurance that transactions are recorded as necessary to permit the preparation of financial statements in conformity with generally accepted accounting principles. If the auditor determines that the deficiency would prevent prudent officials in the conduct of their own affairs from concluding that they have reasonable assurance, then the auditor should deem the deficiency to be at least a significant deficiency. Having determined in this manner that a deficiency represents a significant deficiency, the auditor must further evaluate the deficiency to determine whether individually, or in combination with other deficiencies, the deficiency is a material weakness.

APPENDIX G

SAMPLE DOCUMENTATION

Segment

Division

Location

SEGREGATION OF DUTIES IN SIGNIFICANT ACCOUNTING APPLICATIONS

Adequate segregation of duties reduces the likelihood that errors (intentional or unintentional) will remain undetected by providing for separate processing by different individuals at various stages of a transaction and for independent reviews of the work performed.

A fundamental element of internal control is the segregation of certain key duties. The basic idea underlying segregation of duties is that no employee or group should be in a position both to perpetrate and to conceal errors or fraud in the normal course of their duties. In general, the principal incompatible duties to be segregated are:

- Custody of assets (such as maintenance of check stock)
- Authorization or approval of related transactions affecting those assets (such as the approval of access to vendor master files)
- Recording or reporting of related transactions (such as issuance of purchase orders)
- Verification (control activity such as reconciliation of bank accounts)

An essential feature of segregation of duties/responsibilities within an organization is that no one employee or group of employees has exclusive control over any transaction or group of transactions. In addition, a control

Appendix G

over the processing of a transaction should not be performed by the same individual who is responsible for recording or reporting the transaction.

Based on the above criteria, this form has been designed to highlight conflicting duties performed by one individual (potential lack of proper segregation of duties). This form is completed by indicating the name(s) of the individual(s) responsible for each function within the applications listed. If a function is performed by a computer application, indicate “computer” or “IT” as the “individual.”

After the form has been completed for each significant application, the division finance executive (DFE), controller, or internal control manager (ICM) should review the form for any instances where one individual is performing duties that would be considered to be incompatible. Potential incompatible duties would exist if one individual performs duties in more than one category (authorization or approval, custody, or recording/reporting) or if an individual is responsible for performing a control/verification over the same transaction that the individual is responsible for recording/reporting.

Once an individual is identified as performing incompatible duties, all duties performed by that individual should be considered to determine whether the effectiveness of those duties is reduced or eliminated by the lack of segregation of duties. If it is, the next step is to address their effects on your assessments of the controls over the applications(s) involved and the risk of fraud.

Accounts Payable/Cash Disbursements Process

The duties to be considered in determining the adequacy of segregation of duties among those responsible for Accounts Payable/Cash Disbursements transactions are listed in the chart.

List the names of individuals responsible for particular functions in the column indicated (e.g., the names of the individuals who are responsible for issuing sales orders would fall into the recording column). Review the chart for individuals whose names are listed in more than one column and then make a determination whether that represents a potential lack of segregation of duties.

Sample Documentation

	<i>Authorization</i>	<i>Custody of Assets</i>	<i>Recording</i>	<i>Verification</i>
Issuance of purchase requisitions				
Approval of purchase requisitions				
Issuance of purchase orders				
Approval of access to vendor master files				
Approval of purchase orders				
Approval of access to purchase-related data files				
Preparation/issuance of debit memos to vendors				
Preparation/issuance of receiving reports				
Receipt of goods from vendors				
Matching of invoices to purchase orders and receiving reports				
Coding of account distribution of vendor invoices				
Approval of account distribution of vendor invoices				
Approval of voucher packages for payment				
Preparation of checks				
Signing of checks				
Mailing of checks				
Maintenance of purchases journal				

(continues)

Appendix G

	<i>Authorization</i>	<i>Custody of Assets</i>	<i>Recording</i>	<i>Verification</i>
Maintenance of accounts payable records				
Reconciliation of accounts payable records (or total of unpaid vouchers) to the general ledger				
Control of the accuracy, completeness of, and access to purchases and accounts payable programs and data files				
Maintenance of controlled check stock				
Approval of use of controlled check stock				
Maintenance of signature plate				
Approval of use of signature plate				
Maintenance of cash disbursements journal				
Reconciliation of bank accounts				
Control of the accuracy, completeness of, and access to cash disbursements programs and data files				

Sample Documentation

Additional Considerations

In instances where “computer” or “IT” has been listed as performing a function checked above, consider whether (1) the individuals authorized to enter transactions or adjustments perform other incompatible duties and (2) whether you have procedures to ensure that only authorized individuals have the capabilities to enter the transactions or adjustments.

In addition, when the “computer” or “IT” has been identified as performing *potentially* incompatible duties, consider whether the segregation of duties within the IT department and/or other controls result in effective segregation of duties.

Conclusion

Have any potentially conflicting duties been identified? YES ☐ NO ☐

If potentially conflicting duties have been identified, note them below and indicate their effects on your evaluation of the controls and your assessment of the risk of fraud. If no mitigating controls are in place to offset these conflicting duties, please record your findings in the corrective action log.

Appendix G

FLOWCHART SUPPLEMENTAL NARRATIVES ACCOUNTS PAYABLE/CASH DISBURSEMENTS

Supplemental narratives are provided below to augment the documentation of processes included in the accounts payable/cash disbursements flowcharts. Nonroutine, judgmental, and accounting estimation areas are discussed and references for overlapping areas are given.

Unbilled Receipts/Debit Memos/Rebates from Vendors

Monthly invoices submitted by vendors are matched with the receiving document/bill of lading/traveler and with the original purchase order (three-way match) and entered into the system. Since purchase orders (POs) are not required for expenses such as consulting fees or other services, including utilities, invoices require the approval of applicable supervisors prior to forwarding to the accounts payable department for entry into the system.

Unmatched invoices are placed on hold pending research and resolution of problems by the purchasing department in conjunction with other affected departments. Goods deemed to be damaged upon receipt will be inspected and either scrapped (and removed from inventory), repaired and returned to inventory, or returned to the vendor based on issuance of debit memos, which should match vendor credit memos. Discrepancies in quantities received or price generally result either in debit memos to adjust for lower amounts received/dollars invoiced or modified POs/additional invoices to record higher quantities or prices.

For product/material received for which there is no invoice on hand, the purchasing clerk and/or manager will contact the vendor to initiate immediate completion and issuance of a replacement invoice.

After the problem has been resolved, enabling a successful three-way match, the invoice is entered into the system by the accounts payable (AP) clerk after review/approval by the purchasing manager and the accounting manager. In addition, at the end of each month the accounting manager requests a status report/review from the AP manager of all accruals for goods and services received but not matched with invoices that have yet to be resolved. An aged report of open orders should be researched in detail by the AP clerk and any old/unusual items thoroughly investigated and, if possible, resolved. Issuance of debit memos to adjust for or, if appropriate,

Sample Documentation

write off open items should be prepared by the AP clerk, reviewed by the AP manager, and approved by the accounting manager.

At month end, a summary report comparing receiving and return-to-vendor transactions to invoices and debit memos is prepared and reconciled; any remaining open or problem invoices will be accrued for in the general ledger. The month-end analysis will in particular identify any unusual debit memo transactions during the month that will require further research in the following month for resolution.

Rebates due from suppliers should be identified by the purchasing manager and actively followed up on in accordance with established, valid contractual terms. The purchasing manager should contact the vendor directly to request that the supplier issue a credit memo for any rebates earned; the purchasing manager should also prepare a corresponding debit memo and forward it to the AP clerk for recording of the rebate as an off-set to the outstanding amount payable to that particular vendor. Based on input/analysis from the purchasing manager, the accounting manager will also accrue at the end of each month for any earned rebates due but as yet unprocessed from vendors for which no debit memo has been issued.

Petty Cash

Employees of each business unit/location/department accumulate receipts for allowable reimbursement from the applicable petty cash fund in accordance with the unit's established written policies and procedures with respect to types and dollar limits of small value purchases/expenses incurred. The receipts are then sent to the general ledger (GL) accountant for review and validation. All petty cash reimbursement requests should be written up on a petty cash form and must be properly coded and include the signature of the employee's department manager. Once the form is complete, the GL accountant advances the requested amount to the employee from the petty cash fund, files a copy of the petty cash form as evidence of the disbursement, and posts the transaction to a spreadsheet, denominating the currency and coinage paid out.

The GL accountant audits the fund in accordance with a predetermined schedule or more frequently if replenishment is needed. When replenishment is required, the GL accountant prepares a check request with applicable support, including a reconciliation spreadsheet, supported by receipts, and a breakdown of the requested replenishment by denomination of coins

Appendix G

and bills. The accounting manager reviews and approves the reconciliation prior to replenishment by accounts payable; if discrepancies/shortages are detected, the accounting manager follows up to determine reasons (errors or other) for the shortage and whether a write off is needed. The accounting manager should also perform a surprise audit of the petty cash fund at least twice annually.

Employee Travel Expenses

For employees without travel and expense cards, business travel expenses are to be submitted promptly via travel expense reports in accordance with established written policies and procedures governing allowable travel expenses. After returning from a business trip, the employee compiles all required receipts for reimbursable expenses, codes them to applicable GL accounts, and completes a summary expense report with the appropriate backup for review and approval by his or her department manager. Once approved, the report is forwarded to the AP clerk for processing and audit/verification of the report for accuracy and validity with respect to a preestablished travel expense checklist. The AP clerk then submits the report and backup to the accounting manager for review/approval and return to the AP clerk. The approved expense report is subsequently vouchered and added to the next scheduled regular check run.

Purchase Card Reviews/ Accruals

The principal steps and control points in the purchase card process are detailed on a supplemental flowchart (not included). Several of the steps require management judgment with respect to application of mitigating controls.

At the conclusion of each month, the AP clerk reviews receipts for any unusual purchase card activity and informs the AP manager of his findings. If, in the opinion of the AP manager, any unusual transaction requires further investigation, the following steps should be taken:

- Cardholder is notified of the basis for the manager's concern; additional information may be requested.

Sample Documentation

- AP clerk should conduct further research, if appropriate.
- AP manager advises accounting manager to adjust month end expenses via accrual(s).

Special Handling of Checks

The principal steps and control points in the cash disbursements process are detailed on a supplemental flowchart (not included). Several of the steps require management judgment with respect to application of mitigating controls.

Upon receipt of the system generated list of invoices and the total dollar amount to be paid for the forthcoming check run, the accounting manager and/or controller will review the preliminary check run and earmark any invoices that should be removed for later payment based on special vendor circumstances or cash flow considerations. The AP manager must then reconfirm final invoice selection in the system prior to actual printing of checks.

After the check run is complete, the AP clerk pulls out all checks which require that backup be sent with the remittance; the AP clerk also removes and secures any checks requiring overnight delivery and/or checks identified for subsequent pick up by either the payee or the initiator of the request.

The AP manager similarly pulls out checks requiring dual signature authorization over a specified dollar limit, in accordance with established written guidelines, as well as checks for unrecognizable vendors, voids, or zero dollar value checks. Each of these situations should be thoroughly researched and dispositioned in a timely manner.

TESTING PLAN

Significant Process:
Accounts Payable/Cash Disbursements

Location: Hometown, U.S.

Identification of Significant Controls

<i>Control Number</i>	<i>RFC Number</i>	<i>Primary Control to be Tested</i>	<i>Control Type</i>	<i>Supporting Documents to be Reviewed</i>	<i>Sample Size</i>	<i>Sample Selection Procedures</i>
1	1.1 1.5	Verification and sign-off of purchase requisitions/POs	P	POs/purchase requisitions/invoices—paid and filed	All open/ 36	Verify all open POs/requisitions Avg. 58 POs/mo \times 10% \times 6 mo
2	4.1 6.1 7.1	Three-way match/document match	D	Invoices—paid and filed/PO and non-PO	75	3 yr avg. 237 invoices/mo \times 10% \times 3 mo
3	15.1	Invoice no. previously used for same vendor in GP	D	GP-generated report sorted by invoice number	1	Annual/multiple year invoice print out
4	9.1 10.1 11.1	Check report—review and sign-off for checks needed, issuance of blank stock	P	Aging report (GP generated), check stock log sign off	6	Twice monthly (effective 4/1/04) \times 3 mo Check stock reconciliation
5	2.1	Non-PO invoices are reviewed and approved	P	Invoices—paid and filed	18	Less than 1/2 PO size— 25/mo \times 10% \times 6 mo
6	10.3	Checks are matched with backup	D	Invoices—paid and filed	75	3 yr avg. 237 invoices/mo \times 10% \times 3 mo

7	12.1 12.2	Wires/ACH are reviewed, approved, and released	P	Expense reports/wire forms	30 12	ACH avg. 30/mo × 10% × 6 mo Wire avg. 4/mo × 50% × 6 mo
8	17.1	Expense reports are reviewed and approved	D	Paid expense reports in files	30	Avg. 50/mo × 10% × 6 mo
9	22.1 18.1	Bank/petty cash reconciliations reviewed and approved	P	Reconciliations in files	12 12	Review all monthly reconciliations
10	16.1	Controller AP subledger to GL reconciliation	P	Reconciliations in files	12	Review all monthly reconciliations

Please provide any additional comments related to the establishment of the above Testing Plan:

We have reviewed the Testing Plan shown above and believe that the proposed testing procedures are sufficient to determine the effectiveness of controls within the process.

Process Owner (sign and date)

Controller (sign and date)

Appendix G

INTERNAL CONTROL DOCUMENTATION PROCESS WALK-THROUGH

Segment/Division: _____

Location: _____

Process: _____

Completed by: _____

- I. Describe the procedures performed to confirm your understanding of the process and its control activities:

- II. Provide observations as to the comparison of the process design/documentation to the process execution (include noted gaps, required changes to the documentation):

- III. Provide observations as to occurrence and functionality of process control activities:

- IV. Provide observations as to any internal control weaknesses discovered within the process:

Process Owner

Plant Controller (or equivalent)

INTERNAL CONTROL DOCUMENTATION CORRECTIVE ACTION LOG

SEGMENT/DIVISION: _____ LOCATION: _____
PROCESS: _____ PROCESS OWNER: _____

[illegible]

Signatures below indicate that the items on this log have been reviewed and that the information presented is accurate.

Signature of Process Owner

Date

Signature of Controller

Date

Signature of Division Financial Executive

Date _____

Signature of Segment Financial Executive

Date _____

PARSON CONSULTING INTERNAL CONTROL STRUCTURE AND RISK ASSESSMENT

Inventory Management/Distribution

- Purpose:
 1. Identify "generic" processes within a cycle.
 2. Identify objectives associated with a process.
 3. Identify risk associated with objectives.
 4. Identify "generic" control activities one might find at a client.

#	Process Description	#	Control Objective	#	Risk Consequence	Inherent Risk		Control Description	Financial Assertion	Control Type		
						Financial/Operational Impact	Likelihood Risk			Automated/Manual	Preventive/Detective/Corrective	Primary/Secondary
1	Receiving	1.1	Receiving counts, verifies and agrees information on PO against packing slip or other receiving documents.	1.1.1	Receiving incorrect inventory or received goods that were not authorized or not purchased could result in erroneous payment to vendors.	3– Moderate	2–Low	1.1.1.1	C, V, R	MN	P	S
		1.2	Appropriate monthly cut-off procedures have been established to record receipts into the system timely	1.2.1	Untimely input of receipts or unrecorded receipts may create over-/understatement of inventory balance	3– Moderate	2–Low	1.2.1.1	C, V, R	A	P	PR
		1.3	Restrict access to the system to authorized employees only.	1.3.1	Theft and or fraud of materials and misstatement of inventory records.	3– Moderate	2–Low	1.3.1.1	C, V	MN	P	S
	1.4	Receiving procedures are established to handle discrepancy or issues from incorrect quantities, damaged/defective goods, etc	1.4.1		Damaged/defective goods, inaccurate receipt, etc. can impact inventory valuation, invoice entry, and payment.	3– Moderate	2–Low	1.4.1.1	C, V, R	MN	P	S
								1.4.1.2	C, V, R	MN	P	S
	1.5	Documents of receipts are available for records.	1.5.1		Lack of documents and records for proof of receipts and matching with purchase orders.	3– Moderate	2–Low	1.5.1.1	V, R	MN	D	S
								1.5.1.2	V, R	A	P	S

2	Warehousing	2.1	Incoming goods are properly safeguarded during or after the receipts.	2.1.1	Lack of safeguarding may result in theft. Unsuitable conditions for inventory may result in reduced shelf life or damage.	2– Minor	2–Low	2.1.1.1	Merchandise is safeguarded at their assigned locations and are identifiable.	V, R	MN	P	S
		2.2	Physical access to inventory is restricted	2.2.1	Unauthorized access to inventory at the receiving, storage, or shipping areas may result in fraudulent activities.	2– Minor	2–Low	2.2.1.1	Physical access of inventory is restricted to the DC personnel.	V, R	MN	P	S
		2.3	Inventory movement is properly documented and keep tracked of within the system.	2.3.1	Lack of documentation or tracking of inventory movement may lead to incorrect report of inventory.	2– Minor	2–Low	2.3.1.1	Inventory movement from the receiving dock to secondary location is manually recorded in MINT by the receiving coordinator.	C, V, E	MN	P	PR
								2.3.1.2	Inventory shipped from the DC to stores is tracked by the ASST. VP on a daily basis (i.e., UPS/FedEx sites).	C, V, E	MN	D	S
3	Shipping	2.4	Adequate segregation of duties among shipping, receiving, stocking functions is maintained.	2.4.1	Lack of segregation duties could result in fraudulent activity or loss of materials.	3– Moderate	2–Low		Duties are properly segregated among shipping, receiving, and stocking (refer to the document called Segregation of Duties).				
		3.1	Shipment of inventory is properly authorized.	3.1.1	Move or transfer of inventory without authorization increases errors and potential for loss.	3– Moderate	2–Low	3.1.1.1	Designated inventory levels initiate the movement and transfer of inventory which is entered by buyers.	C, V, E	A	P	S
		3.2	Record transfers and shipments accurately in the system in a timely manner.	3.2.1	Release of inventory without properly recording the event will lead to misstatement of balance sheet and income statement accounts.	3– Moderate	2–Low	3.2.1.1	Outgoing merchandise is scanned, which creates a transactional posting as "Shipped/in-transit" in MINT automatically.	C, V, E	A	P	PR
								3.2.1.2	Received merchandise from DC are entered manually in the system which creates a transactional posting as "Received" into MINT.	C, V, E	MN	P	PR

																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																					</
--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	----

4.5	Adjust inventory status and balances to categorize excess and obsolete materials.	4.5.1	Inappropriate categorization of materials results in financial misstatements.	2— Minor	2—Low	4.5.1.1	Inventory reserves are maintained on the books in a separate inventory account.	C, V	MN	D	S
4.6	Write-off materials identified as obsolete in the GL on a timely basis.	4.6.1	Lack of timely GL adjustment for obsolete inventory results in overstatement of inventory value.	3— Moderate	2—Low	4.6.1.1	A JE is created and recorded for disposed merchandise.	C, V	MN	D	S
4.7	Identify and account for intercompany stock transfers.	4.7.1	Incorrect accounting for profit reconciled between affiliated entities related to intercompany sales.	3— Moderate	2—Low	4.7.1.1	Stock transfers are recorded in MINT when the outgoing or received goods are scanned with the transfer system. After scanning, "confirming" goods scanned adjusts classification.	C, V, E, R	A	P	S
4.8	Perpetual records are validated by an approved cycle count program and an annual physical inventory.	4.8.1	Inaccurate inventory balances may occur when perpetual records are not reconciled to physical counts or quantities on hand.	3— Moderate	2—Low	4.8.1.1	Cycle counts are performed by the DC inventory control dept. periodically throughout the fiscal year.	C, V, E, R	MN	D	S
4.9	Variances identified during cycle/physical count are investigated, resolved and/or properly adjusted for with approval (if necessary).	4.9.1	Discrepancies not recounted, validated, investigated, and/or adjusted may result to inaccurate inventory balances.	3— Moderate	2—Low	4.8.1.2	Full physical inventories are completed on a biannual basis.	C, V, E, R	MN	D	S
						4.9.1.1	Management coordinates the investigation of and reconciliation process of any discrepancies from cycle and full physical inventory counts.	C, V, E, R	MN	D	S
						4.9.1.2	The asst. VP of logistics (cycle counts), CFO (cycle and full physical), and solutions center (full physical) approve any required adjustments to inventory levels.	C, V, E, R	MN	D	PR

Appendix G

Accounts Payable/Cash Disbursements

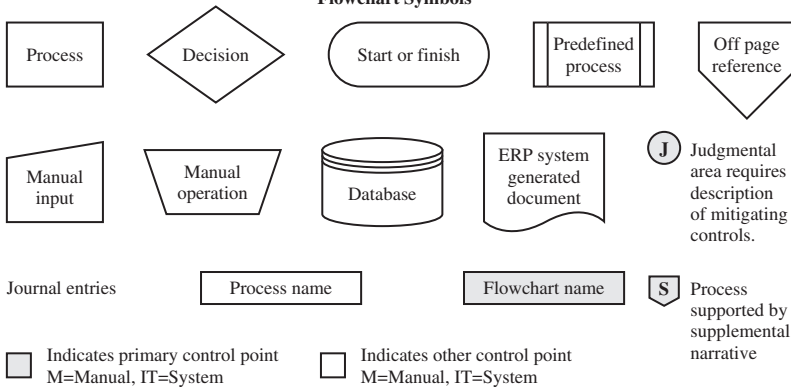
ABC Company
Any segment
Any division
Any location

Process Title Page

Flowcharts Included	Prepared by	Approved by	Revised	Page
Process overview	A.T. Employee	T.P. Controller	04/01/03	2
Purchase requisition/ purchase order	A.T. Employee	T.P. Controller	04/01/03	3
Receiving	A.T. Employee	T.P. Controller	04/01/03	4
Invoice processing	A.T. Employee	T.P. Controller	04/01/03	5
No PO receipt invoices	A.T. Employee	T.P. Controller	04/01/03	6
Cash disbursements	A.T. Employee	T.P. Controller	04/01/03	7
Manual checks	A.T. Employee	T.P. Controller	04/01/03	8
Wire transfer	A.T. Employee	T.P. Controller	04/01/03	9
Purchase cards	A.T. Employee	T.P. Controller	04/01/03	10
Expense reports	A.T. Employee	T.P. Controller	04/01/03	11
Month-end account reconciliations	A.T. Employee	T.P. Controller	04/01/03	12

Legend

Flowchart Symbols



Acromyns

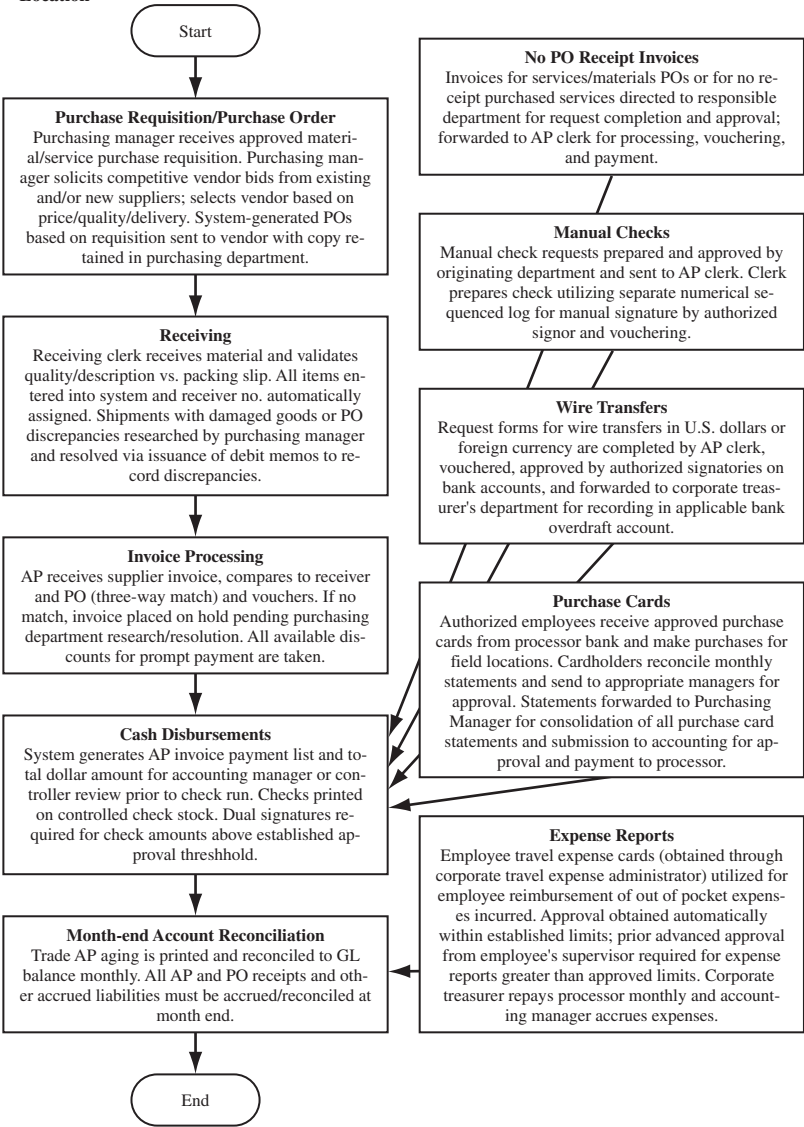
AP -Accounts payable	F/X -Foreign exchange	P Card -Purchase card	\$ -Dollar
DM -Debit memo	GL -General Ledger	PO -Purchase order	TE Admin -Travel expense administrator
ERP -Enterprise resource planning	I/Co -Intercomapny	RFR -Risk factor reference	WT -Wire transfer
	JE -Journal entry		

Sample Documentation

Accounts Payable/Cash Disbursements

ABC Company
Segment
Division
Location

Process Overview

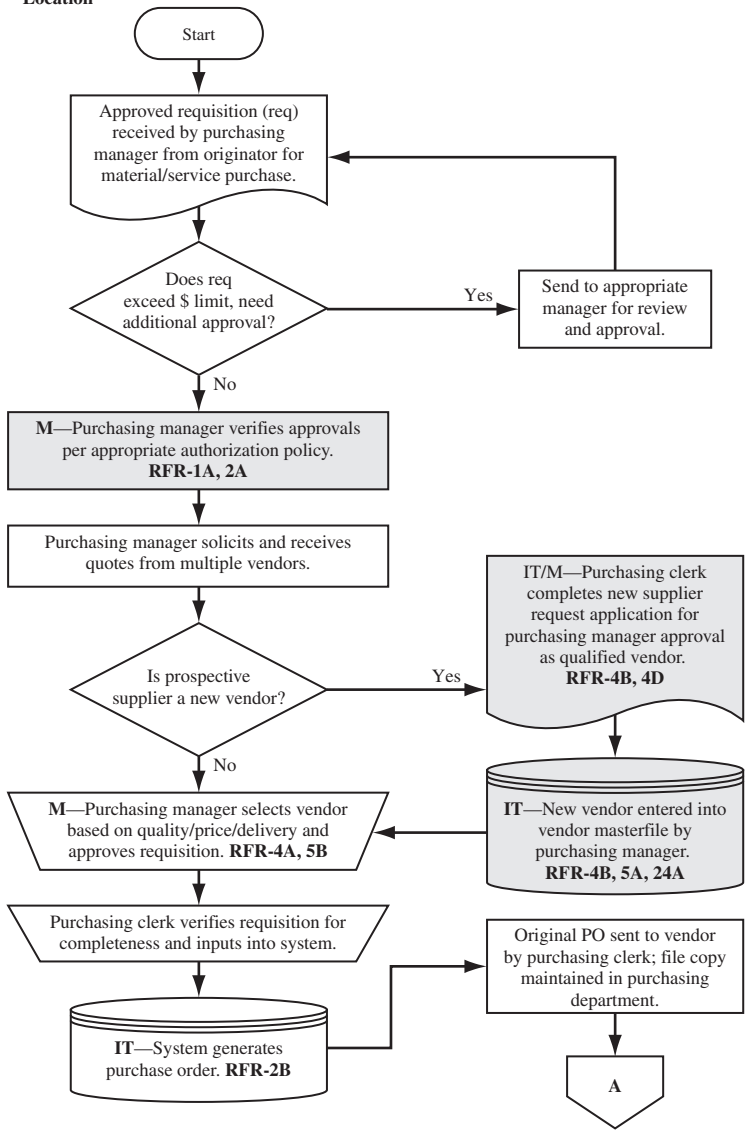


Appendix G

Accounts Payable/Cash Disbursements

ABC Company
Segment
Division
Location

Purchase Requisition/Purchase Order

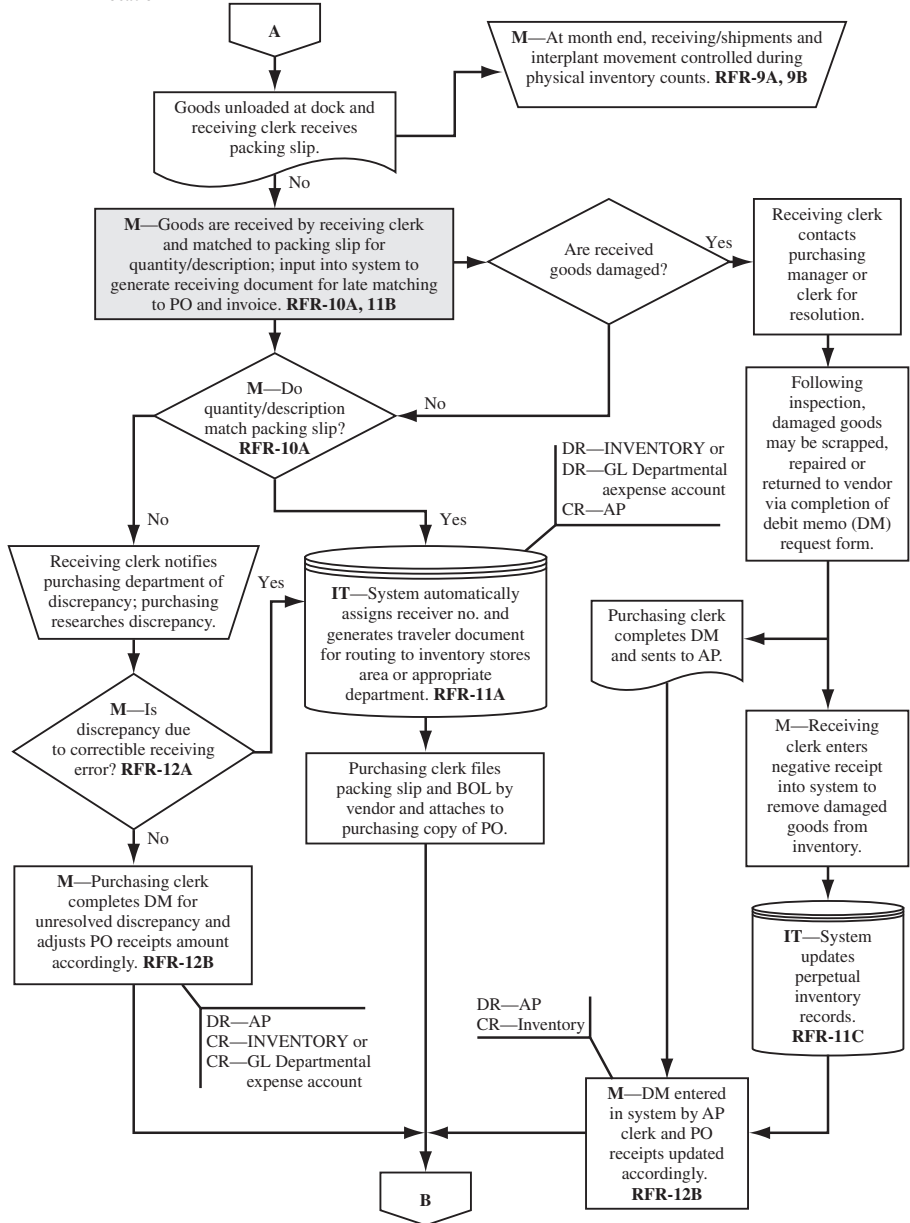


Sample Documentation

Accounts Payable/Cash Disbursements

ABC Company
Segment
Division
Location

Receiving



APPENDIX H

AS2 CONTROL TESTING PROVISIONS¹

TESTING AND EVALUATING DESIGN EFFECTIVENESS

88. Internal control over financial reporting is effectively designed when the controls complied with would be expected to prevent or detect errors or fraud that could result in material misstatements in the financial statements. The auditor should determine whether the company has controls to meet the objectives of the control criteria by:
- Identifying the company's control objectives in each area;
 - Identifying the controls that satisfy each objective; and
 - Determining whether the controls, if operating properly, can effectively prevent or detect errors or fraud that could result in material misstatements in the financial statements.
89. Procedures the auditor performs to test and evaluate design effectiveness include inquiry, observation, walkthroughs, inspection of relevant documentation, and a specific evaluation of whether the controls are likely to prevent or detect errors or fraud that could result in misstatements if they are operated as prescribed by appropriately qualified persons.
90. The procedures that the auditor performs in evaluating management's assessment process and obtaining an understanding of inter-

¹Auditing Standard No. 2. An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements, Paragraphs 88–126, effective pursuant to SEC Release No. 34-49884; File No. PCAOB-2004-03, June 17, 2004.

Appendix H

nal control over financial reporting also provide the auditor with evidence about the design effectiveness of internal control over financial reporting.

91. The procedures the auditor performs to test and evaluate design effectiveness also might provide evidence about operating effectiveness.

TESTING AND EVALUATING OPERATING EFFECTIVENESS

92. An auditor should evaluate the operating effectiveness of a control by determining whether the control is operating as designed and whether the person performing the control possesses the necessary authority and qualifications to perform the control effectively.
93. *Nature of tests of controls.* Tests of controls over operating effectiveness should include a mix of inquiries of appropriate personnel, inspection of relevant documentation, observation of the company's operations, and reperformance of the application of the control. For example, the auditor might observe the procedures for opening the mail and processing cash receipts to test the operating effectiveness of controls over cash receipts. Because an observation is pertinent only at the point in time at which it is made, the auditor should supplement the observation with inquiries of company personnel and inspection of documentation about the operation of such controls at other times. These inquiries might be made concurrently with performing walkthroughs.
94. Inquiry is a procedure that consists of seeking information, both financial and nonfinancial, of knowledgeable persons throughout the company. Inquiry is used extensively throughout the audit and often is complementary to performing other procedures. Inquiries may range from formal written inquiries to informal oral inquiries.
95. Evaluating responses to inquiries is an integral part of the inquiry procedure. Examples of information that inquiries might provide include the skill and competency of those performing the control, the relative sensitivity of the control to prevent or detect errors or fraud, and the frequency with which the control operates to prevent or detect errors or fraud. Responses to inquiries might provide the auditor with information not previously possessed or with corroborative evidence. Alternatively, responses might provide information that

AS2 Control Testing Provisions

differs significantly from other information the auditor obtains (for example, information regarding the possibility of management override of controls). In some cases, responses to inquiries provide a basis for the auditor to modify or perform additional procedures.

96. Because inquiry alone does not provide sufficient evidence to support the operating effectiveness of a control, the auditor should perform additional tests of controls. For example, if the company implements a control activity whereby its sales manager reviews and investigates a report of invoices with unusually high or low gross margins, inquiry of the sales manager as to whether he or she investigates discrepancies would be inadequate. To obtain sufficient evidence about the operating effectiveness of the control, the auditor should corroborate the sales manager's responses by performing other procedures, such as inspecting reports or other documentation used in or generated by the performance of the control, and evaluate whether appropriate actions were taken regarding discrepancies.
97. The nature of the control also influences the nature of the tests of controls the auditor can perform. For example, the auditor might examine documents regarding controls for which documentary evidence exists. However, documentary evidence regarding some aspects of the control environment, such as management's philosophy and operating style, might not exist. In circumstances in which documentary evidence of controls or the performance of controls does not exist and is not expected to exist, the auditor's tests of controls would consist of inquiries of appropriate personnel and observation of company activities. As another example, a signature on a voucher package to indicate that the signer approved it does not necessarily mean that the person carefully reviewed the package before signing. The package may have been signed based on only a cursory review (or without any review). As a result, the quality of the evidence regarding the effective operation of the control might not be sufficiently persuasive. If that is the case, the auditor should reperform the control (for example, checking prices, extensions, and additions) as part of the test of the control. In addition, the auditor might inquire of the person responsible for approving voucher packages what he or she looks for when approving packages and how many errors have been found within voucher packages. The auditor also might inquire of supervisors whether they have any knowledge of

Appendix H

errors that the person responsible for approving the voucher packages failed to detect.

98. *Timing of tests of controls.* The auditor must perform tests of controls over a period of time that is adequate to determine whether, as of the date specified in management's report, the controls necessary for achieving the objectives of the control criteria are operating effectively. The period of time over which the auditor performs tests of controls varies with the nature of the controls being tested and with the frequency with which specific controls operate and specific policies are applied. Some controls operate continuously (for example, controls over sales), while others operate only at certain times (for example, controls over the preparation of monthly or quarterly financial statements and controls over physical inventory counts).
99. The auditor's testing of the operating effectiveness of such controls should occur at the time the controls are operating. Controls "as of" a specific date encompass controls that are relevant to the company's internal control over financial reporting "as of" that specific date, even though such controls might not operate until after that specific date. For example, some controls over the period-end financial reporting process normally operate only after the "as of" date. Therefore, if controls over the December 31, 20X4 period-end financial reporting process operate in January 20X5, the auditor should test the control operating in January 20X5 to have sufficient evidence of operating effectiveness "as of" December 31, 20X4.
100. When the auditor reports on the effectiveness of controls "as of" a specific date and obtains evidence about the operating effectiveness of controls at an interim date, he or she should determine what additional evidence to obtain concerning the operation of the control for the remaining period. In making that determination, the auditor should evaluate:
 - The specific controls tested prior to the "as of" date and the results of those tests;
 - The degree to which evidence about the operating effectiveness of those controls was obtained;
 - The length of the remaining period; and
 - The possibility that there have been any significant changes in internal control over financial reporting subsequent to the interim date.

AS2 Control Testing Provisions

101. For controls over significant nonroutine transactions, controls over accounts or processes with a high degree of subjectivity or judgment in measurement, or controls over the recording of period-end adjustments, the auditor should perform tests of controls closer to or at the “as of” date rather than at an interim date. However, the auditor should balance performing the tests of controls closer to the “as of” date with the need to obtain sufficient evidence of operating effectiveness.
102. Prior to the date specified in management’s report, management might implement changes to the company’s controls to make them more effective or efficient or to address control deficiencies. In that case, the auditor might not need to evaluate controls that have been superseded. For example, if the auditor determines that the new controls achieve the related objectives of the control criteria and have been in effect for a sufficient period to permit the auditor to assess their design and operating effectiveness by performing tests of controls, he or she will not need to evaluate the design and operating effectiveness of the superseded controls for purposes of expressing an opinion on internal control over financial reporting.
103. As discussed in paragraph 207, however, the auditor must communicate all identified significant deficiencies and material weaknesses in controls to the audit committee in writing. In addition, the auditor should evaluate how the design and operating effectiveness of the superseded controls relates to the auditor’s reliance on controls for financial statement audit purposes.
104. *Extent of tests of controls.* Each year the auditor must obtain sufficient evidence about whether the company’s internal control over financial reporting, including the controls for all internal control components, is operating effectively. This means that each year the auditor must obtain evidence about the effectiveness of controls for all relevant assertions related to all significant accounts and disclosures in the financial statements. The auditor also should vary from year to year the nature, timing, and extent of testing of controls to introduce unpredictability into the testing and respond to changes in circumstances. Paragraph 179 provides reporting directions in those circumstances when the auditor has not been able to obtain evidence that the new controls were appropriately designed or have been operating effectively for a sufficient period of time the controls at a

Appendix H

different interim period; increase or reduce the number and types of tests performed; or change the combination of procedures used.

105. In determining the extent of procedures to perform, the auditor should design the procedures to provide a high level of assurance that the control being tested is operating effectively. In making this determination, the auditor should assess the following factors:

- *Nature of the control.* The auditor should subject manual controls to more extensive testing than automated controls. In some circumstances, testing a single operation of an automated control may be sufficient to obtain a high level of assurance that the control operated effectively, provided that information technology general controls also are operating effectively. For manual controls, sufficient evidence about the operating effectiveness of the controls is obtained by evaluating multiple operations of the control and the results of each operation. The auditor also should assess the complexity of the controls, the significance of the judgments that must be made in connection with their operation, and the level of competence of the person performing the controls that is necessary for the control to operate effectively. As the complexity and level of judgment increase or the level of competence of the person performing the control decreases, the extent of the auditor's testing should increase.
- *Frequency of operation.* Generally, the more frequently a manual control operates, the more operations of the control the auditor should test. For example, for a manual control that operates in connection with each transaction, the auditor should test multiple operations of the control over a sufficient period of time to obtain a high level of assurance that the control operated effectively. For controls that operate less frequently, such as monthly account reconciliations and controls over the period-end financial reporting process, the auditor may test significantly fewer operations of the control. However, the auditor's evaluation of each operation of controls operating less frequently is likely to be more extensive. For example, when evaluating the operation of a monthly exception report, the auditor should evaluate whether the judgments made with regard to the disposition of the exceptions were appropriate and adequately supported. Note: When sampling is appropriate and the population of controls to be tested is large,

AS2 Control Testing Provisions

increasing the population size does not proportionately increase the required sample size.

- *Importance of the control.* Controls that are relatively more important should be tested more extensively. For example, some controls may address multiple financial statement assertions, and certain period-end detective controls might be considered more important than related preventive controls. The auditor should test more operations of such controls or, if such controls operate infrequently, the auditor should evaluate each operation of the control more extensively.
106. *Use of professional skepticism when evaluating the results of testing.* The auditor must conduct the audit of internal control over financial reporting and the audit of the financial statements with professional skepticism, which is an attitude that includes a questioning mind and a critical assessment of audit evidence. For example, even though a control is performed by the same employee whom the auditor believes performed the control effectively in prior periods, the control may not be operating effectively during the current period because the employee could have become complacent, distracted, or otherwise not be effectively carrying out his or her responsibilities. Also, regardless of any past experience with the entity or the auditor's beliefs about management's honesty and integrity, the auditor should recognize the possibility that a material misstatement due to fraud could be present. Furthermore, professional skepticism requires the auditor to consider whether evidence obtained suggests that a material misstatement due to fraud has occurred. In exercising professional skepticism in gathering and evaluating evidence, the auditor must not be satisfied with less-than-persuasive evidence because of a belief that management is honest.
107. When the auditor identifies exceptions to the company's prescribed control procedures, he or she should determine, using professional skepticism, the effect of the exception on the nature and extent of additional testing that may be appropriate or necessary and on the operating effectiveness of the control being tested. A conclusion that an identified exception does not represent a control deficiency is appropriate only if evidence beyond what the auditor had initially planned and beyond inquiry supports that conclusion.

USING THE WORK OF OTHERS

108. In all audits of internal control over financial reporting, the auditor must perform enough of the testing himself or herself so that the auditor's own work provides the principal evidence for the auditor's opinion. The auditor may, however, use the work of others to alter the nature, timing, or extent of the work he or she otherwise would have performed. For these purposes, the work of others includes relevant work performed by internal auditors, company personnel (in addition to internal auditors), and third parties working under the direction of management or the audit committee that provides information about the effectiveness of internal control over financial reporting. Note: Because the amount of work related to obtaining sufficient evidence to support an opinion about the effectiveness of controls is not susceptible to precise measurement, the auditor's judgment about whether he or she has obtained the principal evidence for the opinion will be qualitative as well as quantitative. For example, the auditor might give more weight to work he or she performed on pervasive controls and in areas such as the control environment than on other controls, such as controls over low-risk, routine transactions.
109. The auditor should evaluate whether to use the work performed by others in the audit of internal control over financial reporting. To determine the extent to which the auditor may use the work of others to alter the nature, timing, or extent of the work the auditor would have otherwise performed, in addition to obtaining the principal evidence for his or her opinion, the auditor should:
- a. Evaluate the nature of the controls subjected to the work of others (see paragraphs 112 through 116);
 - b. Evaluate the competence and objectivity of the individuals who performed the work (see paragraphs 117 through 122); and
 - c. Test some of the work performed by others to evaluate the quality and effectiveness of their work (see paragraphs 123 through 125). Note: AU sec. 322, *The Auditor's Consideration of the Internal Audit Function in an Audit of Financial Statements*, applies to using the work of internal auditors in an audit of the financial statements. The auditor may apply the relevant concepts

AS2 Control Testing Provisions

described in that section to using the work of others in the audit of internal control over financial reporting.

110. The auditor must obtain sufficient evidence to support his or her opinion. Judgments about the sufficiency of evidence obtained and other factors affecting the auditor's opinion, such as the significance of identified control deficiencies, should be those of the auditor. Evidence obtained through the auditor's direct personal knowledge, observation, reperformance, and inspection is generally more persuasive than information obtained indirectly from others, such as from internal auditors, other company personnel, or third parties working under the direction of management.
111. The requirement that the auditor's own work must provide the principal evidence for the auditor's opinion is one of the boundaries within which the auditor determines the work he or she must perform himself or herself in the audit of internal control over financial reporting. Paragraphs 112 through 125 provide more specific and definitive direction on how the auditor makes this determination, but the directions allow the auditor significant flexibility to use his or her judgment to determine the work necessary to obtain the principal evidence and to determine when the auditor can use the work of others rather than perform the work himself or herself. Regardless of the auditor's determination of the work that he or she must perform himself or herself, the auditor's responsibility to report on the effectiveness of internal control over financial reporting rests solely with the auditor; this responsibility cannot be shared with the other individuals whose work the auditor uses. Therefore, when the auditor uses the work of others, the auditor is responsible for the results of their work.
112. *Evaluating the nature of the controls subjected to the work of others.* The auditor should evaluate the following factors when evaluating the nature of the controls subjected to the work of others. As these factors increase in significance, the need for the auditor to perform his or her own work on those controls increases. As these factors decrease in significance, the need for the auditor to perform his or her own work on those controls decreases. The following factors should be considered:
 - The materiality of the accounts and disclosures that the control addresses and the risk of material misstatement.

Appendix H

- The degree of judgment required to evaluate the operating effectiveness of the control (that is, the degree to which the evaluation of the effectiveness of the control requires evaluation of subjective factors rather than objective testing).
 - The pervasiveness of the control.
 - The level of judgment or estimation required in the account or disclosure.
 - The potential for management override of the control.
113. Because of the nature of the controls in the control environment, the auditor should not use the work of others to reduce the amount of work he or she performs on controls in the control environment. The auditor should, however, consider the results of work performed in this area by others because it might indicate the need for the auditor to increase his or her work.
114. The control environment encompasses the following factors:
- Integrity and ethical values;
 - Commitment to competence;
 - Board of directors or audit committee participation; see the COSO report and paragraph 110 of AU sec. 319, *Internal Control in a Financial Statement Audit*, for additional information about the factors included in the control environment;
 - Management's philosophy and operating style;
 - Organizational structure;
 - Assignment of authority and responsibility; and
 - Human resource policies and procedures.
115. Controls that are part of the control environment include, but are not limited to, controls specifically established to prevent and detect fraud that is at least reasonably possible to result in material misstatement of the financial statements. Note: The term "reasonably possible" has the same meaning as in FAS No. 5. See the first note to paragraph 9 for further discussion.
116. The auditor should perform the walkthroughs (as discussed beginning at paragraph 79) himself or herself because of the degree of judgment required in performing this work. However, to provide additional evidence, the auditor may also review the work of others

AS2 Control Testing Provisions

who have performed and documented walkthroughs. In evaluating whether his or her own evidence provides the principal evidence, the auditor's work on the control environment and in performing walkthroughs constitutes an important part of the auditor's own work.

117. *Evaluating the competence and objectivity of others.* The extent to which the auditor may use the work of others depends on the degree of competence and objectivity of the individuals performing the work. The higher the degree of competence and objectivity, the greater use the auditor may make of the work; conversely, the lower the degree of competence and objectivity, the less use the auditor may make of the work. Further, the auditor should not use the work of individuals who have a low degree of objectivity, regardless of their level of competence. Likewise, the auditor should not use the work of individuals who have a low level of competence regardless of their degree of objectivity.
118. When evaluating the competence and objectivity of the individuals performing the tests of controls, the auditor should obtain, or update information from prior years, about the factors indicated in the following paragraph. The auditor should determine whether to test the existence and quality of those factors and, if so, the extent to which to test the existence and quality of those factors, based on the intended effect of the work of others on the audit of internal control over financial reporting.
119. Factors concerning the competence of the individuals performing the tests of controls include:
 - Their educational level and professional experience.
 - Their professional certification and continuing education.
 - Practices regarding the assignment of individuals to work areas.
 - Supervision and review of their activities.
 - Quality of the documentation of their work, including any reports or recommendations issued.
 - Evaluation of their performance.
120. Factors concerning the objectivity of the individuals performing the tests of controls include:
 - The organizational status of the individuals responsible for the work of others ("testing authority") in testing controls, including—

Appendix H

- a. Whether the testing authority reports to an officer of sufficient status to ensure sufficient testing coverage and adequate consideration of, and action on, the findings and recommendations of the individuals performing the testing.
 - b. Whether the testing authority has direct access and reports regularly to the board of directors or the audit committee.
 - c. Whether the board of directors or the audit committee oversees employment decisions related to the testing authority.
 - Policies to maintain the individuals' objectivity about the areas being tested, including—
 - a. Policies prohibiting individuals from testing controls in areas in which relatives are employed in important or internal control sensitive positions.
 - b. Policies prohibiting individuals from testing controls in areas to which they were recently assigned or are scheduled to be assigned upon completion of their control testing responsibilities.
121. Internal auditors normally are expected to have greater competence with regard to internal control over financial reporting and objectivity than other company personnel. Therefore, the auditor may be able to use their work to a greater extent than the work of other company personnel. This is particularly true in the case of internal auditors who follow the International Standards for the Professional Practice of Internal Auditing issued by the Institute of Internal Auditors. If internal auditors have performed an extensive amount of relevant work and the auditor determines they possess a high degree of competence and objectivity, the auditor could use their work to the greatest extent an auditor could use the work of others. On the other hand, if the internal audit function reports solely to management, which would reduce internal auditors' objectivity, or if limited resources allocated to the internal audit function result in very limited testing procedures on its part or reduced competency of the internal auditors, the auditor should use their work to a much lesser extent and perform more of the testing himself or herself.
122. When determining how the work of others will alter the nature, timing, or extent of the auditor's work, the auditor should assess the interrelationship of the nature of the controls, as discussed in paragraph 112, and the competence and objectivity of those who per-

AS2 Control Testing Provisions

formed the work, as discussed in paragraphs 117 through 121. As the significance of the factors listed in paragraph 112 increases, the ability of the auditor to use the work of others decreases at the same time that the necessary level of competence and objectivity of those who perform the work increases. For example, for some pervasive controls, the auditor may determine that using the work of internal auditors to a limited degree would be appropriate and that using the work of other company personnel would not be appropriate because other company personnel do not have a high enough degree of objectivity as it relates to the nature of the controls.

123. *Testing the work of others.* The auditor should test some of the work of others to evaluate the quality and effectiveness of the work. The auditor's tests of the work of others may be accomplished by either (a) testing some of the controls that others tested or (b) testing similar controls not actually tested by others.
124. The nature and extent of these tests depend on the effect of the work of others on the auditor's procedures but should be sufficient to enable the auditor to make an evaluation of the overall quality and effectiveness of the work the auditor is considering. The auditor also should assess whether this evaluation has an effect on his or her conclusions about the competence and objectivity of the individuals performing the work.
125. In evaluating the quality and effectiveness of the work of others, the auditor should evaluate such factors as to whether the:
 - Scope of work is appropriate to meet the objectives.
 - Work programs are adequate.
 - Work performed is adequately documented, including evidence of supervision and review.
 - Conclusions are appropriate in the circumstances.
 - Reports are consistent with the results of the work performed.
126. The following examples illustrate how to apply the directions discussed in this section:
 - *Controls over the period-end financial reporting process.* Many of the controls over the period-end financial reporting process address significant risks of misstatement of the accounts and disclosures in the annual and quarterly financial statements, may

Appendix H

require significant judgment to evaluate their operating effectiveness, may have a higher potential for management override, and may affect accounts that require a high level of judgment or estimation. Therefore, the auditor could determine that, based on the nature of controls over the period-end financial reporting process, he or she would need to perform more of the tests of those controls himself or herself. Further, because of the nature of the controls, the auditor should use the work of others only if the degree of competence and objectivity of the individuals performing the work is high; therefore, the auditor might use the work of internal auditors to some extent but not the work of others within the company.

- *Information technology general controls.* Information technology general controls are part of the control activities component of internal control; therefore, the nature of the controls might permit the auditor to use the work of others. For example, program change controls over routine maintenance changes may have a highly pervasive effect, yet involve a low degree of judgment in evaluating their operating effectiveness, can be subjected to objective testing, and have a low potential for management override. Therefore, the auditor could determine that, based on the nature of these program change controls, the auditor could use the work of others to a moderate extent so long as the degree of competence and objectivity of the individuals performing the test is at an appropriate level. On the other hand, controls to detect attempts to override controls that prevent unauthorized journal entries from being posted may have a highly pervasive effect, may involve a high degree of judgment in evaluating their operating effectiveness, may involve a subjective evaluation, and may have a reasonable possibility for management override. Therefore, the auditor could determine that, based on the nature of these controls over systems access, he or she would need to perform more of the tests of those controls himself or herself. Further, because of the nature of the controls, the auditor should use the work of others only if the degree of competence and objectivity of the individuals performing the tests is high.
- *Management self-assessment of controls.* As described in paragraph 40, management may test the operating effectiveness of controls using a self-assessment process. Because such an assessment

AS2 Control Testing Provisions

is made by the same personnel who are responsible for performing the control, the individuals performing the self-assessment do not have sufficient objectivity as it relates to the subject matter. Therefore, the auditor should not use their work.

- *Controls over the calculation of depreciation of fixed assets.* Controls over the calculation of depreciation of fixed assets are usually not pervasive, involve a low degree of judgment in evaluating their operating effectiveness, and can be subjected to objective testing. If these conditions describe the controls over the calculation of depreciation of fixed assets and if there is a low potential for management override, the auditor could determine that, based on the nature of these controls, he or she could use the work of others to a large extent (perhaps entirely) so long as the degree of competence and objectivity of the individuals performing the test is at an appropriate level.
- *Alternating tests of controls.* Many of the controls over accounts payable, including controls over cash disbursements, are usually not pervasive, involve a low degree of judgment in evaluating their operating effectiveness, can be subjected to objective testing, and have a low potential for management override. When these conditions describe the controls over accounts payable, the auditor could determine that, based on the nature of these controls, he or she could use the work of others to a large extent (perhaps entirely) so long as the degree of competence and objectivity of the individuals performing the test is at an appropriate level. However, if the company recently implemented a major information technology change that significantly affected controls over cash disbursements, the auditor might decide to use the work of others to a lesser extent in the audit immediately following the information technology change and then return, in subsequent years, to using the work of others to a large extent in this area. As another example, the auditor might use the work of others for testing controls over the depreciation of fixed assets (as described in the point above) for several years' audits but decide one year to perform some extent of the work himself or herself to gain an understanding of these controls beyond that provided by performing a walk-through.

**EXAMPLE D-1. SIGNIFICANT DEFICIENCIES
AND MATERIAL WEAKNESSES²**

Paragraph 8 of this standard defines a control deficiency. Paragraphs 9 and 10 go on to define a significant deficiency and a material weakness, respectively.

- Paragraphs 22 through 23 of this standard discuss materiality in an audit of internal control over financial reporting, and paragraphs 130 through 140 provide additional direction on evaluating deficiencies in internal control over financial reporting.
- The following examples illustrate how to evaluate the significance of internal control deficiencies in various situations. These examples are for illustrative purposes only.

**EXAMPLE D-1. RECONCILIATIONS OF INTERCOMPANY
ACCOUNTS ARE NOT PERFORMED ON A TIMELY BASIS**

Scenario A. Significant Deficiency

The company processes a significant number of routine intercompany transactions on a monthly basis. Individual intercompany transactions are not material and primarily relate to balance sheet activity, for example, cash transfers between business units to finance normal operations. A formal management policy requires monthly reconciliation of intercompany accounts and confirmation of balances between business units. However, there is not a process in place to ensure performance of these procedures. As a result, detailed reconciliations of intercompany accounts are not performed on a timely basis. Management does perform monthly procedures to investigate selected large-dollar intercompany account differences. In addition, management prepares a detailed monthly variance analysis of operating expenses to assess their reasonableness. Based only on these facts, the auditor should determine that this deficiency represents a significant deficiency for the following reasons: The magnitude of a financial statement misstatement resulting from this deficiency would reasonably be

²*Id.*, Appendix D.

AS2 Control Testing Provisions

expected to be more than inconsequential, but less than material, because individual intercompany transactions are not material, and the compensating controls operating monthly should detect a material misstatement. Furthermore, the transactions are primarily restricted to balance sheet accounts. However, the compensating detective controls are designed only to detect material misstatements. The controls do not address the detection of misstatements that are more than inconsequential but less than material. Therefore, the likelihood that a misstatement that was more than inconsequential, but less than material, could occur is more than remote.

Scenario B. Material Weakness

The company processes a significant number of intercompany transactions on a monthly basis. Intercompany transactions relate to a wide range of activities, including transfers of inventory with intercompany profit between business units, allocation of research and development costs to business units, and corporate charges. Individual intercompany transactions are frequently material. A formal management policy requires monthly reconciliation of intercompany accounts and confirmation of balances between business units. However, there is not a process in place to ensure that these procedures are performed on a consistent basis. As a result, reconciliations of intercompany accounts are not performed on a timely basis, and differences in intercompany accounts are frequent and significant. Management does not perform any alternative controls to investigate significant intercompany account differences. Based only on these facts, the auditor should determine that this deficiency represents a material weakness for the following reasons: The magnitude of a financial statement misstatement resulting from this deficiency would reasonably be expected to be material, because individual intercompany transactions are frequently material and relate to a wide range of activities. Additionally, actual unreconciled differences in intercompany accounts have been, and are, material. The likelihood of such a misstatement is more than remote because such misstatements have frequently occurred and compensating controls are not effective, either because they are not properly designed or not operating effectively. Taken together, the magnitude and likelihood of misstatement of the financial statements resulting from this internal control deficiency meet the definition of a material weakness.

**EXAMPLE D-2. EVALUATE IMPACT ON TIMING AND
AMOUNT OF REVENUE RECOGNITION**

Scenario A. Significant Deficiency

The company uses a standard sales contract for most transactions. Individual sales transactions are not material to the entity. Sales personnel are allowed to modify sales contract terms. The company's accounting function reviews significant or unusual modifications to the sales contract terms, but does not review changes in the standard shipping terms. The changes in the standard shipping terms could require a delay in the timing of revenue recognition. Management reviews gross margins on a monthly basis and investigates any significant or unusual relationships. In addition, management reviews the reasonableness of inventory levels at the end of each accounting period. The entity has experienced limited situations in which revenue has been inappropriately recorded in advance of shipment, but amounts have not been material. Based only on these facts, the auditor should determine that this deficiency represents a significant deficiency for the following reasons: The magnitude of a financial statement misstatement resulting from this deficiency would reasonably be expected to be more than inconsequential, but less than material, because individual sales transactions are not material and the compensating detective controls operating monthly and at the end of each financial reporting period should reduce the likelihood of a material misstatement going undetected. Furthermore, the risk of material misstatement is limited to revenue recognition errors related to shipping terms as opposed to broader sources of error in revenue recognition. However, the compensating detective controls are only designed to detect material misstatements. The controls do not effectively address the detection of misstatements that are more than inconsequential but less than material, as evidenced by situations in which transactions that were not material were improperly recorded. Therefore, there is a more than remote likelihood that a misstatement that is more than inconsequential but less than material could occur.

Scenario B. Material Weakness

The company has a standard sales contract, but sales personnel frequently modify the terms of the contract. The nature of the modifications can affect

AS2 Control Testing Provisions

the timing and amount of revenue recognized. Individual sales transactions are frequently material to the entity, and the gross margin can vary significantly for each transaction. The company does not have procedures in place for the accounting function to regularly review modifications to sales contract terms. Although management reviews gross margins on a monthly basis, the significant differences in gross margins on individual transactions make it difficult for management to identify potential misstatements. Improper revenue recognition has occurred, and the amounts have been material. Based only on these facts, the auditor should determine that this deficiency represents a material weakness for the following reasons: The magnitude of a financial statement misstatement resulting from this deficiency would reasonably be expected to be material, because individual sales transactions are frequently material, and gross margin can vary significantly with each transaction (which would make compensating detective controls based on a reasonableness review ineffective). Additionally, improper revenue recognition has occurred, and the amounts have been material. Therefore, the likelihood of material misstatements occurring is more than remote. Taken together, the magnitude and likelihood of misstatement of the financial statements resulting from this internal control deficiency meet the definition of a material weakness.

Scenario C. Material Weakness

The company has a standard sales contract, but sales personnel frequently modify the terms of the contract. Sales personnel frequently grant unauthorized and unrecorded sales discounts to customers without the knowledge of the accounting department. These amounts are deducted by customers in paying their invoices and are recorded as outstanding balances on the accounts receivable aging. Although these amounts are individually insignificant, they are material in the aggregate and have occurred consistently over the past few years. Based on only these facts, the auditor should determine that this deficiency represents a material weakness for the following reasons: The magnitude of a financial statement misstatement resulting from this deficiency would reasonably be expected to be material, because the frequency of occurrence allows insignificant amounts to become material in the aggregate. The likelihood of material misstatement of the financial statements resulting from this internal control deficiency is more than remote (even assuming that the amounts were fully

Appendix H

reserved for in the company's allowance for uncollectible accounts) due to the likelihood of material misstatement of the gross accounts receivable balance. Therefore, this internal control deficiency meets the definition of a material weakness.

EXAMPLE D-3. IDENTIFICATION OF SEVERAL DEFICIENCIES

Scenario A. Material Weakness

During its assessment of internal control over financial reporting, management identified the following deficiencies. Based on the context in which the deficiencies occur, management and the auditor agree that these deficiencies individually represent significant deficiencies:

- Inadequate segregation of duties over certain information system access controls.
- Several instances of transactions that were not properly recorded in subsidiary ledgers; transactions were not material, either individually or in the aggregate.
- A lack of timely reconciliations of the account balances affected by the improperly recorded transactions.

Based only on these facts, the auditor should determine that the combination of these significant deficiencies represents a material weakness for the following reasons: Individually, these deficiencies were evaluated as representing a more than remote likelihood that a misstatement that is more than inconsequential, but less than material, could occur. However, each of these significant deficiencies affects the same set of accounts. Taken together, these significant deficiencies represent a more than remote likelihood that a material misstatement could occur and not be prevented or detected. Therefore, in combination, these significant deficiencies represent a material weakness.

Scenario B. Material Weakness

During its assessment of internal control over financial reporting, management of a financial institution identifies deficiencies in the design of

AS2 Control Testing Provisions

controls over the estimation of credit losses (a critical accounting estimate); the operating effectiveness of controls for initiating, processing, and reviewing adjustments to the allowance for credit losses; and the operating effectiveness of controls designed to prevent and detect the improper recognition of interest income. Management and the auditor agree that, in their overall context, each of these deficiencies individually represents a significant deficiency. In addition, during the past year, the company experienced a significant level of growth in the loan balances that were subjected to the controls governing credit loss estimation and revenue recognition, and further growth is expected in the upcoming year. Based only on these facts, the auditor should determine that the combination of these significant deficiencies represents a material weakness for the following reasons:

- The balances of the loan accounts affected by these significant deficiencies have increased over the past year and are expected to increase in the future.
- This growth in loan balances, coupled with the combined effect of the significant deficiencies described, results in a more than remote likelihood that a material misstatement of the allowance for credit losses or interest income could occur. Therefore, in combination, these deficiencies meet the definition of a material weakness.

APPENDIX I

RESPONSIBILITIES OF INTERNAL AUDITING

The purpose of this statement is to provide in summary form a general understanding of the responsibilities of internal auditing. For more specific guidance, readers should refer to the *Standards for the Professional Practice of Internal Auditing*.

OBJECTIVE AND SCOPE

Internal auditing is an independent appraisal function especially established within an organization to examine and evaluate its activities as a service to the organization. The objective of internal auditing is to assist members of the organization in the effective discharge of their responsibilities. To this end, internal auditing furnishes them with analyses, appraisals, recommendations, counsel, and information concerning the activities reviewed. The audit objective includes promoting effective control at reasonable cost. The members of the organization assisted by internal auditing include those in management and the board of directors.

The scope of internal auditing should encompass the examination and evaluation of the adequacy and effectiveness of the organization's system of internal control and the quality of performance in carrying out assigned responsibilities. Internal auditors should:

- Review the reliability and integrity of financial and operating information and the means used to identify, measure, classify, and report such information.
- Review the systems established to ensure compliance with those policies, plans, procedures, laws, and regulations, which could have

Appendix I

a significant impact on operations and reports, and should determine whether the organization is in compliance.

- Review the means of safeguarding assets and, as appropriate, verify the existence of such assets.
- Appraise the economy and efficiency with which resources are employed.
- Review operations or programs to ascertain whether results are consistent with established objectives and goals and whether the operations or programs are being carried out as planned.

RESPONSIBILITIES AND AUTHORITY

The internal auditing department is an integral part of the organization and functions under the policies established by senior management and the board. The purpose, authority, and responsibility of the internal auditing department should be defined in a formal written document (charter). The director of internal auditing should seek approval of the charter by senior management as well as acceptance by the board. The charter should make clear the purposes of the internal auditing department, specify the unrestricted scope of its work, and declare that auditors are to have no authority or responsibility for the activities they audit.

Throughout the world, internal auditing is performed in diverse environments and within organizations that vary in purpose, size, and structure. In addition, the laws and customs within various countries differ from one another. These differences may affect the practice of internal auditing in each environment. The implementation of the *Standards for the Professional Practice of Internal Auditing*, therefore, will be governed by the environment in which the internal auditing department carries out its assigned responsibilities. Compliance with the concepts enunciated by the *Standards for the Professional Practice of Internal Auditing* is essential before the responsibilities of internal auditors can be met. As stated in the Code of Ethics, members of the Institute of Internal Auditors, Inc. and Certified Internal Auditors shall adopt suitable means to comply with the *Standards for the Professional Practice of Internal Auditing*.

INDEPENDENCE

Internal auditors should be independent of the activities they audit. Internal auditors are independent when they can carry out their work freely and objectively. Independence permits internal auditors to render the impartial and unbiased judgments essential to the proper conduct of audits. It is achieved through organizational status and objectivity.

The organizational status of the internal auditing department should be sufficient to permit the accomplishment of its audit responsibilities. The director of the internal auditing department should be responsible to an individual in the organization with sufficient authority and independence to ensure a broad audit coverage, adequate consideration of audit reports, and appropriate action on audit recommendations.

The organizational status of the internal auditing department should be sufficient to permit the accomplishment of its audit responsibilities. The director of the internal auditing department should be responsible to an individual in the organization with sufficient authority to promote independence and to ensure a broad audit coverage, adequate consideration of audit reports, and appropriate action on audit recommendations.

Objectivity is an independent mental attitude that internal auditors should maintain in performing audits. Internal auditors are not to subordinate their judgment on audit matters to that of others. Designing, installing, and operating systems are not audit functions. Also, the drafting of procedures for systems is not an audit function. Performing such activities is presumed to impair audit objectivity.

APPENDIX J

ACTUAL INTERNAL CONTROL DISCLOSURES¹

<i>Company</i>	<i>Date</i>	<i>Description</i>
Fisher Communications Inc. —Television station group. <u>2003 Sales:</u> \$138.4 million <u>Auditor:</u> Pricewaterhouse-Coopers	Aug. 26	STEPS TAKEN TO CORRECT MATERIAL WEAKNESS —We have assigned the highest priority to the correction of this deficiency and have taken and will continue to take action to fully correct it . . . As of August 2004 we have taken the following corrective action: <ul style="list-style-type: none"> • In August 2003, we hired a Vice President of Finance. • In October 2003, we engaged independent consulting firm to assist the company with compliance under Section 404 of the Sarbanes-Oxley Act of 2002 and related Securities and Exchange Commission rules. • In October 2003, we established the policy and practice that our Vice President of Finance prepare a memorandum that identified significant transactions which had occurred during the recent quarterly period, document appropriate accounting treatment and financial statement disclosure for such transactions, and distribute the memorandum to senior management, the independent auditors, and the audit committee for review and comment. • In early November 2003, we commenced use of a new disclosure and control procedures checklist in connection with preparation of our financial statements and our periodic reports.

¹Compliance Week, *Internal Control Disclosures in August: Remediation*, September 8, 2004, obtained from the Compliance Week web site: www.complianceweek.com.

Appendix J

<i>Company</i>	<i>Date</i>	<i>Description</i>
		<ul style="list-style-type: none"> • In November 2003, with the assistance of an independent consulting firm, we began the process of evaluating compliance under Section 404 of the Sarbanes-Oxley Act of 2002 and related Securities and Exchange Commission rules. • In December 2003, we hired a new staff accountant. • In January 2004, we hired an additional controller. • In February 2004, we hired an internal control analyst. • In February 2004, we established a practice that significant one-time transactions be reviewed and evaluated by both the chief financial officer and the vice president of finance (or other appropriate senior accounting staff member) to determine appropriate accounting treatment and financial statement disclosure. • In April 2004, we hired a director of financial planning and analysis. • In connection with the preparation of the company's quarterly report on Form 10-Q for the fiscal quarter ended March 31, 2004, the company implemented a practice whereby the company's senior financial personnel increased communication with managers at operating sites with regard to the financial statement close process and disclosure matters. • In April 2004 we announced the retirement of David Hillard as chief financial officer and the appointment of Robert Bateman as his successor. • In June 2004, we hired a new Vice President of Finance to replace Robert Bateman, who was appointed chief financial officer.
QuadraMed Corp. —Health care management software provider. 2003 Sales: \$125.1 million	Aug. 25	UPDATE ON PAST WEAKNESS —The company has now implemented procedures to report movements in deferred revenue on an overall roll forward basis. We are also in the process of upgrading our computer software, which is expected to be completed in the second half of 2004. The company believes that the costs associated with implementing these processes and computer software to be immaterial.

Actual Internal Control Disclosures

<i>Company</i>	<i>Date</i>	<i>Description</i>
<p><u>Auditor:</u> BDO Seidman</p>		<p>In its report, BDO also identified the following reportable conditions related to:</p> <ul style="list-style-type: none"> • Internal controls over analysis and review of customer contracts • The revenue transactions cycle • Unbilled and deferred revenue balances • Percentage of completion revenue recognition <p>The company is addressing these items by implementing the following procedures:</p> <ul style="list-style-type: none"> • Documenting the formal review of contracts in the determination of proper revenue accounting • Redesigning the contracting process and review procedures • Upgrading computer software relating to contracts and billing • Strengthening documentation standards and maintaining detailed historical records for each customer for revenue recognition
<p>Southwall Technologies Inc.—Plastic & fiber manufacturer.</p> <p><u>2003 Sales:</u> \$53.3 million</p> <p><u>Auditor:</u> Pricewaterhouse-Coopers</p>	Aug. 23	<p>MATERIAL WEAKNESSES IDENTIFIED— . . . These material weaknesses were caused by a reduction in force that occurred during 2002 and 2003 and related to the inadequacy of review and supervision of the preparation of accounting records and the untimely reconciliation of certain accounts. The audit committee of the company's board of directors discussed such material weaknesses with PwC. The company has taken steps to attempt to improve its internal controls and its control environment. The company has hired a new corporate controller, a new director of financial planning and analysis, a new senior cost accountant, and a new senior accountant for the company's Germany subsidiary; appointed a new plant manager for the company's U.S. manufacturing operations; initiated retraining of personnel on the correct use of the company's new ERP system; initiated procedures to attempt to ensure all accounts are reconciled and reviewed on a timely basis; and, is in the process of documenting its procedures and reviewing its internal controls to ensure compliance under section 404 of the Sarbanes-Oxley Act. The company has authorized PwC to respond fully to inquiries of the successor</p>

Appendix J

<i>Company</i>	<i>Date</i>	<i>Description</i>
		independent accountants concerning such material weaknesses.
Interpool Inc.— Container leasing company. <u>2003 Sales:</u> \$375.6 million <u>Auditor:</u> KPMG	Aug. 18	UPDATE ON PAST CONTROLS WEAKNESSES —We, in conjunction with our independent auditors, KPMG, identified certain material weaknesses within our system of internal control. We noted that formal procedures were not in place that required management to properly communicate the terms of proposed transactions with internal and external technical accounting resources to make certain that transactions are accounted for in accordance with accounting principles generally accepted in the United States. In addition, we noted that we did not have an individual with the proper level of understanding to account for swap derivatives according to accounting principles generally accepted in the United States. In response to these weaknesses, we: <ul style="list-style-type: none"> • Initiated regular meetings of senior management, including the chief financial officer and representatives of the accounting department, to discuss all new significant transactions in order to determine the proper accounting treatment under accounting principles generally accepted in the United States • Retained the services of a consultant to assist in the proper documentation and accounting for swap derivative transactions In addition, our general counsel, who was not located in our executive offices in New York, NY, or Princeton, NJ, was not always informed about, and was inconsistently consulted regarding, factual and legal issues critical to our compliance with securities laws and accounting rules. We also concluded that we were late in responding to warning signs pointing to inadequate staffing and controls in our accounting department and inadequate information systems capabilities, even though members of our audit committee had repeatedly urged management to respond to these problems.

Actual Internal Control Disclosures

<i>Company</i>	<i>Date</i>	<i>Description</i>
<p>Lifeway Foods Inc.— Dairy products company.</p> <p><u>2003 Sales:</u> \$14.9 million</p> <p><u>Auditor:</u> Plante & Moran</p>	Aug. 16	<p>CONTROLS IMPROVEMENTS MADE— . . . The company has historically operated on strictly monitored cost constraints; with that perspective, the chief executive officer concluded that the disclosure controls and procedures are effective in ensuring that all material information required to be filed in this quarterly report has been made known to her. However, based on the company's recent growth and improved cash position, as well as consultation with its auditors, management intends to implement additional procedures to improve internal controls in 2004. Specifically, an enhanced accounting software package has been identified that will permit enhanced data recording and internal reporting as well as additional on-site accounting staff and some changes to internal control procedures.</p>
<p>Nui Corp.— Natural gas company.</p> <p><u>2003 Sales:</u> \$652.4 million</p> <p><u>Auditor:</u> Pricewaterhouse- Coopers</p>	Aug. 16	<p>REMEDIATION EFFORTS UNDERWAY—The company has undertaken a long-term effort to assess our systems of internal control and to comply with the requirements of Section 404 of the Sarbanes-Oxley Act. These actions include:</p> <ul style="list-style-type: none"> • Performing a comprehensive evaluation and developing a remediation plan with respect to internal controls over financial reporting and related processes • Implementing a redesigned cash management process and adopting more stringent cash management practices and procedures • Developing and implementing comprehensive accounting and financial reporting policies and procedures • Implementing procedures for performance of account analyses and reconciliations • Improving and monitoring controls to increase the reliability of information generated by our information technology processes • Educating employees throughout the company as to the importance of compliance with policies and procedures and the significance of a system of sound internal controls

Appendix J

<i>Company</i>	<i>Date</i>	<i>Description</i>
		<ul style="list-style-type: none"> Ensuring executive management's involvement in the oversight and review of the disclosure and reporting process
Evans & Sutherland Computer Corp.— Industrial & military computer systems. <u>2003 Sales:</u> \$84.8 million <u>Auditor:</u> KPMG	Aug. 16	IMPROVEMENTS TO MATERIAL WEAKNESS —As a result of our findings described above, during the first quarter of 2004, we implemented the following improvements to our internal control procedures and our disclosure controls and procedures to address the issues we identified in our evaluation of these controls and procedures and those of our subsidiary, E&S Ltd. We altered our reporting structure so that the finance director of E&S Ltd. reports directly to our chief financial officer; we appointed a director of internal control whose primary responsibilities are to oversee the establishment of formalized policies and procedures throughout our organization and to document and assess our system of internal controls; we instituted new procedures around our quarterly reporting processes whereby significant accounting issues are discussed and documented, reviewed with our external auditors and the audit committee, formally approved by our management, and given timely effect in our books and records. In addition, during the second quarter of 2004, we implemented and continue to implement the following improvements to our internal control procedures and our disclosure controls and procedures to address the issues we identified in our evaluation of these controls and procedures and those of our subsidiary, E&S Ltd. We continue to establish new internal control processes to remedy the problems identified; we continue to examine our procedures for quarter-end analysis of balance sheet and income statement accounts, period-end reconciliations of subsidiary ledgers, and the correction of reconciling items in a timely manner. In those areas where we identify weaknesses, we address with specific action items designed to eliminate the weaknesses. We also continue to enhance our accounting documentation policies; we are implementing the financial controls and procedures employed by E&S at our subsidiary, E&S Ltd., whereby monthly sales audit schedules are reconciled to the general ledger; we have begun

Actual Internal Control Disclosures

<i>Company</i>	<i>Date</i>	<i>Description</i>
		reconciling, on a monthly basis, operational assessments of the status of completion of each contract program and the financial accounting and reporting of such status.
Ebix Inc.— Insurance broker. <u>2003 Sales:</u> \$14.4 million <u>Auditor:</u> KPMG	Aug. 16	<p>REPORTABLE CONDITIONS BELIEVED CORRECTED—In connection with the audit of our consolidated financial statements for the year ended December 31, 2003, KPMG advised the company's management and audit committee of reportable conditions related to its internal controls. KPMG presented to the audit committee details of the reportable conditions noted during the 2003 audit, which included delegation of authority, formalized contract review process to ensure proper revenue recognition, accounting for income taxes, analysis/documentation for unusual transactions, and Sarbanes-Oxley 404 internal control matters (documented and testable control environment).</p> <p>In response to KPMG's identified issues, in the first quarter of 2004, the company changed its reporting structure within the financial accounting group and will redistribute responsibilities among the financial accounting group to create improved checks and balances. The responsibility for a formalized contract review process to ensure proper revenue recognition will be reassigned to a financial department director. The ongoing quarterly review of the provision for income taxes will be performed by the chief financial officer, corporate controller, and a newly hired senior financial accounting member located in Australia. The foregoing individuals will also be responsible for the analysis and documentation of any unusual transactions. The company has hired an additional senior staff professional for the financial accounting group whose duties will include Sarbanes-Oxley 404 documentation of internal control matters.</p>
Shurgard Storage Centers Inc.— Industrial REIT. <u>2003 Sales:</u> \$252.9 million	Aug. 13	<p>ACTIONS TAKEN ON REPORTABLE CONDITIONS—The deficiencies in the internal control structure have been discussed among management, our independent auditors, and our audit committee. We assigned the highest priority to the correction of these deficiencies and have taken actions to correct them, including the following:</p>

Appendix J

<i>Company</i>	<i>Date</i>	<i>Description</i>
<u>Auditor:</u> Deloitte & Touche		<ul style="list-style-type: none"> • Appointed an interim chief financial officer in January 2004 and reassigned the former chief financial officer to other responsibilities • Appointed an interim chief accounting officer in January 2004 with substantial public company finance and accounting experience • Hired a chief information officer in January 2004 • Appointed to the board and the audit committee in January 2004 an additional financial expert who has more than 25 years of audit experience with a nationally recognized auditing firm • Engaged in mid-2003 a management consulting firm specializing in internal control documentation and testing to review the company's financial controls and compliance policies • Engaged additional accounting staff beginning in mid-2003 and continuing into 2004, which individuals have experience in financial reporting • Increased training of our corporate and accounting staff to heighten awareness among corporate and accounting personnel of generally accepted accounting principles • Hired a director of internal audit in May 2004 • Hired a chief financial officer designate in May 2004 • Engaged a nationally recognized law firm to conduct a review of our corporate governance, including our compliance with recent regulations arising out of the Sarbanes-Oxley Act of 2002
Transaction Systems Architects Inc.— Develops e-commerce software that facilitates “e-payments.” <u>2003 Sales:</u> \$277.3 million <u>Auditor:</u> KPMG	Aug. 11	UPDATE ON PAST REPORTABLE CONDITION —Improvements in the company's internal controls over financial reporting related to the noted deficiencies have been implemented during the first nine months of fiscal 2004, and corrective actions have been initiated to address any deficiencies outstanding at June 30, 2004 KPMG has advised the audit committee that these internal control deficiencies constitute reportable conditions and, collectively, a material weakness as defined in Statement of Auditing Standards No. 60. Certain of these internal control weaknesses may also indicate deficiencies in the company's disclosure controls. The company has established substantial

Actual Internal Control Disclosures

<i>Company</i>	<i>Date</i>	<i>Description</i>
		<p>additional procedures designed to ensure that these internal control deficiencies do not lead to material misstatements in its consolidated financial statements. . . . In connection with the requirements of Section 404 of the Sarbanes-Oxley Act, the company has commenced documentation and evaluation of its internal controls over financial reporting and has retained consultants to assist in this process. The company will continue to evaluate the effectiveness of its disclosure controls and internal controls and procedures on an ongoing basis, taking corrective action as appropriate.</p>
<p>Pride International Inc.—Energy & utilities.</p> <p>2003 Sales: \$1.6 billion</p> <p><u>Auditor:</u> Pricewaterhouse-Coopers</p>	Aug. 10	<p>REMEDIATION EFFORTS MENTIONED IN “RISK FACTORS” SECTION OF MD&A— Beginning with our report for the year ending December 31, 2004, Section 404</p> <p>of the Sarbanes-Oxley Act of 2002 will require us to include an internal control report of management with our annual report on Form 10-K, which is to include management’s assessment of the effectiveness of our internal control over financial reporting as of the end of the fiscal year. That report will also be required to include a statement that our independent auditors have issued an attestation report on management’s assessment of our internal control over financial reporting. Our independent auditors, Pricewaterhouse-Coopers, issued a letter to our audit committee dated August 13, 2003, noting certain matters in our technical services segment that they considered to be a material weakness in internal control.</p> <p>In order to achieve compliance with Section 404 within the prescribed period, management has formed an internal control steering committee, engaged outside consultants, and adopted a detailed project work plan to assess the adequacy of our internal control over financial reporting, remediate any control weaknesses that may be identified, validate through testing that controls are functioning as documented, and implement a continuous reporting and improvement process for internal control over financial reporting. We may not, however, be able to complete the work necessary for our management to issue its management report in a timely manner, or any</p>

Appendix J

<i>Company</i>	<i>Date</i>	<i>Description</i>
		work that will be required for our management to be able to report that our internal control over financial reporting is effective. In addition, our independent auditors may not be able to issue an attestation report on management's assessment.
Black Box Corp.— Computer products & support company. <u>2004 Sales:</u> \$520.4 million <u>Auditor:</u> Ernst & Young	Aug. 10	UPDATE TO PREVIOUSLY REPORTED REPORTABLE CONDITIONS— The matters involving reportable conditions and other internal control deficiencies have been discussed in detail among management, the audit committee of the company's board of directors, and E&Y. Management will evaluate the specific reportable conditions and other internal control deficiencies identified by E&Y and will develop, in consultation with E&Y and under the direction of the audit committee, measures to enhance internal control systems and procedures. The company is taking actions to permit it to comply timely with Section 404 of the Sarbanes-Oxley Act with respect to its internal control over financial reporting for fiscal year 2005, including the engagement of another independent accounting firm to assist it with respect to Sarbanes-Oxley 404 compliance measures, has added additional accounting resources, plans to establish an internal audit function reporting to the audit committee, and will take such other remedial measures that may be recommended by the audit committee. In addition to increased oversight by the audit committee, the board of directors has appointed a nonexecutive chairman of the board, as previously disclosed, and has nominated for election to the board of directors an individual who has significant public accounting experience.
Mirant Corp.— Wholesale energy marketer. <u>2003 Sales:</u> \$5.2 billion <u>Auditor:</u> KPMG	Aug. 9	REPORTABLE CONDITIONS ADDRESSED, BUT NOT IN DETAIL— As disclosed in previous filings, during 2002, our independent auditors identified a material control weakness related primarily to our North America energy marketing operations. Additionally, since 2002, we have identified various reportable conditions related to our structure of internal control over financial reporting. In order to address the above noted material weakness and reportable conditions, the company implemented

Actual Internal Control Disclosures

<i>Company</i>	<i>Date</i>	<i>Description</i>
		various procedures to mitigate the possibility of material error affecting the financial reporting process. We believe that all identified internal control deficiencies were mitigated in preparing this quarterly report.
Epicor Software Corp. —Enterprise resource planning software company. <u>2003 Sales:</u> \$153.2 million <u>Auditor:</u> KPMG	Aug. 9	PAST REPORTABLE CONDITIONS BELIEVED CORRECTED —Both prior to and following the completion of the merger, both Scala and the company took immediate actions to resolve the issues identified with respect to Scala’s internal and disclosure controls. Specifically, Scala began implementing additional improvements to its financial reporting systems and controls, including evaluating the staffing of its finance and financial reporting department, increasing the training of its finance personnel with respect to U.S. generally accepted accounting principles, and adopting new policies and procedures, including with respect to the documentation of decisions of the Scala managing and supervisory boards. Furthermore, Epicor, as a U.S. publicly traded corporation, possesses extensive experience in operating in an Securities and Exchange Commission reporting environment and extensive accounting and financial resources devoted to such operations. Following the completion of the merger, these Epicor resources were immediately applied to and assumed direct responsibility for reviewing and overseeing Scala’s financials as well as Scala’s financial controls environment. Concurrently, Epicor has imposed its own system of internal controls and processes and procedures as to, among other things, Scala’s licensing, contracting, and revenue recognition procedures and policies in order to bring them into conformance with Epicor’s own policies and procedures. Additionally, immediately following the merger, Scala’s management and supervisory boards were reconstituted to include a majority of Epicor executives familiar with proper record keeping and disclosure controls pertaining to board decisions and the timely reporting of all board commitments and resolutions. The Scala boards also now ultimately report up into the Epicor board structure and, as such,

Appendix J

<i>Company</i>	<i>Date</i>	<i>Description</i>
		<p>the management and supervisory board decisions are not only regularly reviewed and documented, but are subject to Epicor board approval.</p> <p>As of June 30, 2004, the company feels that it has adequately and fully responded to the deficiencies identified by Scala's independent auditors with respect to Scala's internal and disclosure controls. However, in the longer term, as Epicor continues the process of integrating Scala's operations into Epicor's, Epicor plans on continuing to review and, as needed, modify both its own and Scala's internal and disclosure controls procedures in order to ensure the veracity and integrity of the combined companies financial control environment. In that regard, the entire Epicor and Scala operations are currently undergoing an extensive review of their internal controls by an outside and independent big four accounting firm whose review is designed in part to identify and remedy any unknown deficiencies or weaknesses that may be found to exist in Epicor or Scala's internal controls. The ultimate goal of such review includes ensuring that the company is in full compliance with the mandates of Section 404 of the Sarbanes-Oxley legislation on or before December 31, 2004.</p>
<p>Fisher Communications Inc.—Television station group.</p> <p><u>2003 Sales:</u> \$138.4 million</p> <p><u>Auditor:</u> Pricewaterhouse-Coopers</p>	Aug. 9	<p>RISK FACTORS DESCRIBE ACTIONS TAKEN To CORRECT WEAKNESS— . . . In connection with the audit of our financial statements for fiscal 2003, our independent auditors informed management and our audit committee that, taken together, the number of adjustments that were identified indicate the lack of an effective monitoring and oversight function during fiscal 2003, and concluded that this was a significant deficiency in our internal control structure, which they considered to be a material weakness under the then current accounting standards. We have taken actions to correct this material weakness. In particular, we have, among other things (1) increased our finance staff; (2) begun the process of evaluating compliance under Section 404 of the Sarbanes-Oxley Act of 2002 and related rules; (3) commenced the use of a new disclosure and control procedure checklist in connection with preparation of our financial statements and periodic reports; and (4)</p>

Actual Internal Control Disclosures

<i>Company</i>	<i>Date</i>	<i>Description</i>
		established a practice regarding review and evaluation of significant one-time transactions.
aaiPharma Inc. —Pharmaceutical manufacturer. <u>2003 Sales:</u> \$225 million <u>Auditor:</u> Ernst & Young	Aug. 9	STEPS TAKEN TO CORRECT PAST WEAKNESSES — . . . In light of the foregoing, the company has taken the following actions after the end of 2003 to address the deficiencies as described above: <ul style="list-style-type: none"> • During the first quarter of 2004, contracted with a third-party consulting group, FTI Consulting, to provide transitional management services in the area of operations and finance. • During the first quarter of 2004, reassigned all financial controllers from operating units into the finance department reporting to the company's controller and chief accounting officer who reports directly to the chief financial officer. • Commenced a company-wide education effort regarding our code of conduct and contract-approval policies, training 420 employees during the second quarter of 2004. • Implemented a more rigorous contract-approval process during the second quarter of 2004 wherein all divisions affected by a contract must approve of the final draft prior to execution. • Implemented formal revenue recognition protocols and training programs. In addition to a more rigorous examination of revenue recognition under generally accepted accounting principles and applicable Securities and Exchange Commission regulations, these protocols provide that the level of channel inventory and demand trends for products be considered in the analysis of revenue reserves for product sales. Key members of management and finance have been involved in development of these protocols. The company intends to complete training of other employees during the third quarter of 2004. • Initiated process enhancements to the customer credit approval process, which the company intends to complete during the third quarter of 2004. • Initiated improvements to the budgeting and forecasting process, which the company intends to complete during the third quarter of 2004.

Appendix J

<i>Company</i>	<i>Date</i>	<i>Description</i>
		<p>In addition, since December 31, 2003, the company's then chief executive officer, chief operating officer, and chief financial officer have left the company. In March of 2004, Dr. Sancilio, the company's executive chairman and chief scientific officer, was appointed chief executive officer, and Gregory F. Rayburn, a senior managing director with FTI Consulting, was appointed interim chief operating officer. In April 2004, Timothy R. Wright was appointed president of the company's pharmaceuticals products Division. Gina Gutzeit, a senior managing director with FTI Consulting, was appointed as interim chief financial officer in May 2004.</p> <p>The company is fully committed to implementing controls identified by the company's independent auditors and the special committee. The company's efforts to strengthen its financial and internal controls continue, and the company expects to complete remediation of the material weaknesses and reportable condition identified by its independent auditors by the end of 2004 . . .</p>
<p>SOLA International Inc.—Medical equipment & supply company.</p> <p><u>2003 Sales:</u> \$562.7 million</p> <p><u>Auditor:</u> Pricewaterhouse-Coopers</p>	Aug. 9	<p>STEPS TAKEN TO CORRECT PAST WEAKNESSES—We have assigned a high priority to the short-term and long-term improvement of our internal controls over financial reporting. The process began last October 2003 with plans presented by our chief financial officer, who joined SOLA last September, to the board of directors to improve internal controls and financial reporting. We believe that we have developed a plan that addresses the material weakness in our internal controls that should provide for adequate financial reporting in future periods.</p> <p>To date, we have implemented internal control improvements by first strengthening our monitoring controls over the company. For example, we implemented detailed line item reviews with country controllers and corporate staff in the second quarter of fiscal 2004. Other actions we have put in place include implementing more rigorous documentation of accounting issues and creating an audit checklist for country controllers. We have relocated and integrated our North American accounting group with our</p>

Actual Internal Control Disclosures

<i>Company</i>	<i>Date</i>	<i>Description</i>
		<p>corporate accounting group to achieve better connectivity between regional accounting and corporate consolidation and analysis. We have also taken other actions focused on improving timeliness and accuracy of reporting financial information from entities globally.</p> <p>In addition to the foregoing action, we have implemented the process of:</p> <ul style="list-style-type: none"> • Engaging outside consultants to supplement our internal tax staff • Requiring reporting of monthly/quarterly tax liabilities by our country controllers • Establishing a tax audit checklist for our country controllers • Identifying and analyzing process and staffing improvements related to interaction of our corporate accounting and finance group with our regional accounting and finance groups • Adding three CPA positions at corporate accounting, including a director of internal audit and related staff, which we completed during the quarter ended June 30, 2004 • Restructuring management reporting to require detailed variance reporting tied to our plan and our prior year, as well as the identification of quarterly risks and opportunities <p>Also, we consider the implementation of Sarbanes-Oxley Section 404 to be part of our plan to improve controls and are well into the implementation, including expenditures of approximately of \$2.5–\$3.5 million anticipated in fiscal 2005. We are using outside resources combined with internal resources to achieve implementation. The steps we have taken to date and the steps we are still in the process of implementing are subject to continuing management review and testing by our internal and external auditors. We will use our best efforts to meet the compliance requirements of Section 404 of the Sarbanes-Oxley Act; however, given the effort needed to fully comply with the Sarbanes-Oxley Act, we may not be able to take all actions required by the March 31, 2005 deadline.</p>

Appendix J

<i>Company</i>	<i>Date</i>	<i>Description</i>
<p>Captaris Inc.— Messaging, conferencing & communications software.</p> <p><u>2003 Sales:</u> \$83.3 million</p> <p><u>Auditor:</u> Deloitte & Touche</p>	Aug. 9	<p>STEPS TAKEN TO CORRECT PAST WEAKNESSES—. . . The company has made and will continue to make, improvements to its policies, procedures, systems and staff who have significant roles in internal control to address the internal control deficiencies identified by D&T. Key improvements include hiring a new chief financial officer and corporate controller in the third and fourth quarters of 2003, respectively, and other financial staff in the fourth quarter of 2003 and the first six months of 2004. The company will continue to improve and enhance the design of control processes and procedures, and to upgrade staff to strengthen internal controls. In addition, the company implemented its enterprise reporting system in its Australian and Netherlands subsidiaries during the first six months of 2004. As of April 30, 2004, the entire company began operating under one worldwide accounting system. The steps being taken to correct the weaknesses and deficiencies identified by D&T constitute changes that materially affected the company's internal control over financial reporting during the most recent fiscal quarter.</p>
<p>Calpine Corp.— Energy trading & marketing.</p> <p><u>2003 Sales:</u> \$8.9 billion</p> <p><u>Auditor:</u> Pricewaterhouse- Coopers</p>	Aug. 9	<p>DESIGN DEFICIENCIES ADDRESSES—. . . Additionally, the company has completed the process of correcting these design deficiencies by taking the following steps:</p> <ul style="list-style-type: none"> • Manual procedures have been replaced with system-based controls to ensure proper segregation of duties and documentation of approval for the journal entry and vendor maintenance processes • System access rights for financial system software updates have been redefined and restricted to segregate certain activities and allow user activities to be monitored <p>The company continues to test the effectiveness of these changes.</p>
<p>California Micro Devices— Semiconductor company.</p>	Aug. 6	<p>STATUS OF PRIOR WEAKNESSES UPDATED IN "RISK FACTORS"—. . . While preparing our financial statements for the 2003 fiscal year, both our internal staff and prior outside accountants found errors in certain primary financial processes, which</p>

Actual Internal Control Disclosures

<i>Company</i>	<i>Date</i>	<i>Description</i>
<p>2004 Sales: \$59.6 million</p> <p><u>Auditor:</u> Grant Thornton</p>		<p>they corrected during such preparation. However, these errors caused inaccuracies in the fiscal 2003 interim results for the three-, six-, and nine-month periods that required these interim period results to be restated. As a result, our prior outside accountants informed us that they had noted a combination of reportable conditions that, taken together, constituted a material weakness in our internal controls. The material weakness included issues with our inventory costing systems and procedures, accounts payable cutoff, information systems user administration, and finance organization. We have instituted additional processes and procedures to mitigate the conditions identified and to provide reasonable assurance that our internal control objectives are met. During fiscal 2004, we recruited an almost entirely new finance department and we have instituted back-up procedures for our manual processes as we automate them, although some key controls remain manual and are consequently inefficient. We have devoted substantial effort and resources to improving our internal controls, and in connection with our fiscal 2004 audit our current auditors (who were engaged on December 15, 2003, after our prior accountants had resigned on October 14, 2003) did not note and inform us of any reportable condition or material weakness as to our internal controls. We are continuing our efforts to improve and automate our financial processes and procedures; however, there can be no assurance that we will nonetheless have a material error in our financial statements.</p>
<p>Electronic Data Systems Corp.— IT services.</p> <p>2003 Sales: \$21.4 billion</p> <p><u>Auditor:</u> KPMG</p>	Aug. 6	<p>DEFICIENCY IN MAY ALREADY ADDRESSED BY AUGUST—In April 2004, management identified a significant deficiency in the NMCI contract’s purchasing and accrual process associated with certain hardware and subcontractor work-in-progress during 2003. This deficiency resulted in the untimely recognition of the purchase of certain hardware and assets under construction and is also considered to be a reportable condition due to the size of the NMCI contract. Management has implemented measures to improve controls over this process, including centralized approval of all contract-related purchases, monthly subcontractor reporting of work-in-progress</p>

Appendix J

<i>Company</i>	<i>Date</i>	<i>Description</i>
		activities, and increased operational monitoring and reporting of subcontractor activities, and is in the process of implementing an automated warehouse management system. Management believes the measures implemented in the second quarter of 2004 have adequately addressed this deficiency such that it no longer exists.
Foamex —Industrial manufacturer. <u>2003 Sales:</u> \$1.3 billion <u>Auditor:</u> Deloitte & Touche	Aug. 6	STEPS TAKEN TO CORRECT PAST REPORTABLE CONDITIONS —Management of Foamex L.P., under the guidance of the Foamex international audit committee, is in the process of remediating the reportable conditions. Foamex L.P. continues to install a new enterprise-wide information technology system. Foamex L.P. expects to substantially complete the implementation during 2006. Several modules of the system have already been installed and others are currently in the process of being implemented. Foamex L.P. believes it has addressed and remediated the information technology security issues. Foamex L.P. has implemented improved inventory procedures and processes at each of its facilities and is taking appropriate actions to ensure their effectiveness, including training of personnel and additional management oversight. Foamex L.P. performs monthly physical counts and reconciliations of inventory at each of its plants and will continue to do so until perpetual inventory records are available as manufacturing modules of the enterprise-wide information technology system are implemented at its facilities. The inventory procedures are formally documented and include requirements that account reconciliations are reviewed monthly and a checklist of the tasks performed are prepared and reviewed monthly. Foamex L.P. has strengthened and continues to address the controls over the preparation of its quarterly financial reports, including more extensive and stringent analytical review procedures applied to its results as well as developing task logs and checklists to facilitate the accuracy and completeness of its financial statements and required disclosures. Foamex L.P. has codified and standardized closing journal entries across its facilities and has formalized the review and approval process

Actual Internal Control Disclosures

<i>Company</i>	<i>Date</i>	<i>Description</i>
		for such journal entries. Additionally, Foamex L.P. has implemented a standardized consolidation and reporting system in the United States, Mexico and Canada . . .
Alpharma Inc. —Pharmaceutical manufacturer. 2003 Sales: \$1.2 billion <u>Auditor:</u> Pricewaterhouse-Coopers	Aug. 5	STEPS TAKEN; LISTED AS RISK FACTORS ADDED TO ANNUAL REPORT IN 8-K FILING —The company has addressed the reportable conditions by (1) enhancing its overall control environment through extensive changes in USHP leadership, including the appointment of a new President and a new chief financial officer in June 2003, appointing a new Vice President of Supply Chain and business segment leaders in January 2004, and appointing a new controller in April 2004; (2) reorganizing USHP finance and recruiting additional finance personnel; (3) establishing a new position—director, internal controls and compliance—responsible for monitoring internal controls in the USHP division; (4) completing a review of significant balance sheet accounts; and (5) continuously assessing risks via newly established business and financial review processes within the USHP division In addition, in order to achieve compliance with Section 404 of the Sarbanes-Oxley Act within the prescribed period, the company has been engaged since 2003 in a process to document and evaluate its internal controls over financial reporting. In this regard, management has dedicated internal resources, engaged outside consultants and adopted a detailed work plan to (1) assess and document the adequacy of internal control over financial reporting, (2) take steps to improve control processes where appropriate, (3) validate through testing that controls are functioning as documented, and (4) implement a continuous reporting and improvement process for internal control over financial reporting.
Iomega Corp. —Personal storage drives. 2003 Sales: \$391.3 million	Aug. 5	STEPS TAKEN TO CORRECT PAST REPORTABLE CONDITION —As previously discussed in the company’s quarterly report on Form 10-Q for the quarter ended March 28, 2004, during the first quarter of 2004, the company’s independent auditors for the year ended December 31, 2003,

Appendix J

<i>Company</i>	<i>Date</i>	<i>Description</i>
<u>Auditor:</u> Ernst & Young		<p>notified the company's audit committee that they had identified a reportable condition regarding the company's internal controls. The condition, which was not a material weakness, related to the controls around the preparation of the fourth quarter 2003 tax provision, which the company believed was particularly complex due, in part, to the tax consequences of a \$75 million intercompany dividend required to fund the one-time \$5 per share cash dividend paid to shareholders on October 1, 2003. In the first quarter of 2004, the company extended by one week the time between fiscal quarter end and the time that it publicly announces financial results for the completed quarter to allow for further review and analysis of financial results and tax provisions before their disclosure. Also, during the second quarter of 2004, the company further added an additional layer of review by hiring an independent third party to review the quarterly tax provision. The company believes that these actions adequately address the condition.</p>
QuadraMed Corp. —Health care management software. 2003 Sales: \$125.1 million <u>Auditor:</u> BDO Seidman	Aug. 4	<p>STEPS TAKEN TO CORRECT PAST WEAKNESS— . . . The company has now implemented procedures to report movements in deferred revenue on an overall roll forward basis. We are also in the process of upgrading our computer software, which is expected to be completed in the second half of 2004. The company believes that the costs associated with implementing these processes and computer software to be immaterial. . . . The company has addressed these [additional] items by implementing the following procedures:</p> <ul style="list-style-type: none"> • Documenting the formal review of contracts in the determination of proper revenue accounting • Redesigning the contracting process and review procedures • Upgrading computer software relating to contracts and billing • Strengthening documentation standards for revenue recognition for percentage completion revenue accounting

Actual Internal Control Disclosures

<i>Company</i>	<i>Date</i>	<i>Description</i>
Homestore Inc. —Internet content provider. <u>2003 Sales:</u> \$218.7 million <u>Auditor:</u> Ernst & Young	Aug. 4	<p>REPORTABLE CONDITIONS BEING ADDRESSED—. . . As part of the assessment of our internal controls, with the assistance of outside consultants, we continue to review, evaluate, and remediate our internal processes in order to strengthen and establish greater uniformity in their application. As a result of these steps, we intend to continue to refine our internal control processes on an ongoing basis. With respect to the financial close process, we have reviewed key procedures and have realigned those procedures to improve the efficiency and accuracy of the process as well as provide enhanced evidence of timely reconciliations and reviews.</p> <p>During the second quarter of 2004, we implemented certain modules of PeopleSoft financials in conjunction with the first phase of a company-wide enterprise resource planning initiative. In connection therewith, we have updated our internal controls over financial reporting as necessary to accommodate any modifications to our internal processes and accounting procedures, including the improvement and retention of documentation of all accounting policies and procedures as well as all of management’s key assumptions, estimates and conclusions that affect its recorded balances in its financial statements.</p>

INDEX

- Acquisitions, 138
- Adelphia, 3, 12
- American Stock Exchange (Amex), 3
- Analyst conflicts of interest (Title 5), 5
- Analytical and consultative services, 150–151
- Anti-Kickback Act of 1986, 11
- Arthur Andersen, 3
- Attestation engagement, 64, 111
- Audit committee, 13–14
- Audit function considerations, 117–131
 - role of internal audit department, 117–122
 - role of external auditor, 122–130
- Auditing Standard No. 2, 42–49, 123–124, 126–129
 - control deficiency, 44
 - control testing provisions, 219–239
 - internal control over financial reporting, 43–44
 - materiality, 47
 - material weakness, 45–46
 - relevant assertions, 47–48
 - significant account, 47
 - significant deficiency, 44–45
 - significant process, 48–49
- Auditor independence (Title 2), 4
- Basel II, 176–177
- Boards of directors, 13
- Business size, 138–142
- Business strategy, 150
- Canadian Securities Administrators, 174
- Certification reports, 66, 115
- Change management, 71–89
 - failure of change initiatives, 75–78
 - implementation framework, 84–89
 - build, 86
 - design, 86
 - implement, 87
 - plan, 86
 - sustain, 87
 - integrated, 81–89
 - key criteria for success, 78–80
 - readiness for change, 73–75
- Chief executive officer (CEO), 5, 17
- Chief financial officer (CFO), 5, 17
- Collins, Jim, 150
- Commission resources and authority (Title 6), 6
- Committee of European Securities Regulators (CESR), 155
- Committee of Sponsoring Organizations (COSO), 9, 41, 179
 - internal controls approach, 9–11
- Compliance
 - considerations prior to implementation, 33–38
 - cost of, 30–31
 - implementation challenges, 38–40
 - Path to Compliance, 41–68
 - program planning, 50–51
 - scope of compliance program, 31–33

Index

- Compliance activities, ongoing, 91–116
 - improvement opportunities and remediation efforts, 91–94
 - internal control self-assessments, 100
 - monitoring, 98–100
 - operational structures, 95–96
 - Path to Ongoing Act Compliance, 96–116
 - step 1: plan, 101–104
 - step 2: ongoing documentation, 104–106
 - step 3: test, 107–113
 - step 4: remediation, 113–114
 - step 5: report, 114–116
 - process owners, 101
 - role of finance, 94–95
 - tone of executive management, 100–101
 - training and education, 101
- Compliance issues, ongoing, 133–142
 - business size, 138–142
 - information technology (IT) system implementations, 136–138
 - mergers and acquisitions, 138
 - software applications to assist with compliance efforts, 133–136
- Compliance planning, ongoing, 103
- Control deficiency, 44
 - evaluating, 193–195
- Control environment risk assessment, 53–54
- Control Objectives for Information and Related Technology (COBIT), 179
- Control processes, evaluation questions, 189
- Control testing plan, 60–62, 107–110
- Corporate and Criminal Accountability Act of 2002, 6
- Corporate and criminal fraud
 - accountability (Title 8), 6
- Corporate fraud accountability (Title 11), 7
- Corporate Fraud Accountability Act of 2002, 7
- Corporate responsibility (Title 3), 4–5
- Corporate tax returns (Title 10), 6
- Corrective action logs, 58–59
- Cost of compliance, 14–15
- Cultural change and process approach, 148–149
- Defense Industry Initiative (DII) on Business Ethics and Conduct, 11
- Documentation, 54–56
 - ongoing, 104–105
 - sample, 197–217
 - standardization, 56, 105–106
- Donaldson, William, 145, 147
- Enhanced financial disclosures (Title 4), 5
- Enron, 3, 12, 146
- European Commission, 155
- European Union (EU), 155, 173
- Evidential documentation, 64, 112
- Executive management, 14
- External auditors, 14, 52
 - attestation, 66–67, 115
 - considerations, 103–104
 - role of, 122–130
 - testing, 64–65, 112
- Finance strategy, 150
- Financial Executives International (FEI), 15, 30
- Financial manager, 15
- Financial services compliance initiatives, 173–182
 - effective compliance to deliver business value, 180–182
- Sarbanes-Oxley and equivalent
 - legislation, 174–180
 - Basel II, 176–177
 - International Financial Reporting Standards, 175–176
 - Solvency II, 177–180
- Form 8-K, 24–26, 31
- Gap analysis, 56, 106
- General Accounting Office (GAO), 6

Index

- Generally accepted accounting principles (GAAP), 9, 19, 43
- Good to Great: Why Some Companies Make the Leap . . . And Others Don't* (Collins), 149
- Information technology (IT) system implementations, 136–138
- Institute of Chartered Accountants (Ireland), 175
- Integrated change management (ICM), 81
- Internal audit department, 117–122
 - responsibilities of, 241–243
- Internal control culture approach, 147–148
- Internal control disclosures, actual
 - company reports, 245–265
- Internal control over financial reporting, 43–44, 191
- Internal controls environment, 9–12
- Internal testing, 110–111
- International Accounting Standards Board (IASB), 157, 173, 175
- International Financial Reporting Standards (IFRS), 9, 155–165, 173, 175–176
 - accounting issue, 157
 - business issue, 158
 - communicating the impact, 156–157
 - key elements of effective IFRS implementation, 163–165
 - agree upon deliverables, 164
 - ensure board-level buy in, 163
 - set if IFRS transition team, 163–164
 - step away from detail, 165
 - people issue, 158–159
 - preparing for, 159–163
 - Step 1: plan, 160
 - Step 2: analyze, 160–161
 - Step 3: design, 161
 - Step 4: build and implement, 162
 - Step 5: sustain, 162–163
 - systems and processes issues, 157
- Investment Company Act of 1940, 22
- Investors, 12–13
- Management and staff, 14
- Management certifications, 66, 115
- Management testing, 62–64
- Materiality, 47
- Material weakness, 45–46
- Mergers, 138
- Nasdaq Stock Market (Nasdaq), 3
- Necessary cost of doing business approach, 146
- New York Stock Exchange (NYSE), 3
- Non-U.S.-based companies and compliance, 167–172
 - companies affected by Sarbanes-Oxley, 167–168
 - company leaders and Sarbanes-Oxley, 168–169
 - preparation to ensure compliance, 169–172
 - assess existing internal control environment, 170–171
 - build compelling business case, 169–170
 - certify with confidence and avoid prosecution, 172
 - establish internal control framework, 170
 - implement remediation/improvements options, 171
 - responsibility for monitoring, 171–172
- Organizational readiness, 29–40
- Path to Compliance, 41–68
 - Auditing Standard No. 2, 42–49
 - Step 1: plan, 49–52
 - Step 2: review, 52–57
 - Step 3: improve control environment, 57–60
 - Step 4: test, 60–65
 - Step 5: certify, 65–67
 - Step 6: monitor, 67
 - Process change options, 57–58

Index

- Process efficiency opportunities, 58
- Process improvement considerations,
 - 145–154
 - implementation philosophies, 145–149
 - cultural change and process approach, 148–149
 - internal control culture approach, 147–148
 - necessary cost of doing business approach, 146
 - unnecessary burden approach, 146
 - process improvement, 149–153
 - four steps for financial managers, 150–153
- Project charter, 50
- Project steering committee, 49–50,
 - 101–103
- Project team, 50
- Public Company Accounting Oversight Board (PCCOB) (Title 1), 4, 16,
 - 29, 137
 - Auditing Standard No. 2, 42–49
- Quest for Excellence, A*, 11
- Regulatory bodies, 13
- Relevant assertions, 47–48
- Remediation, 113–114
- Sarbanes-Oxley Act of 2002, overview of,
 - 3–16
 - cost of compliance, 14–15
 - effects on participants in financial reporting process, 12–14
 - audit committee, 13–14
 - boards of directors, 13
 - executive management, 14
 - external auditors, 14
 - investors and other users of financial data, 12–13
 - management and staff, 14
 - regulatory bodies, 13
 - internal controls environment, 9–12
 - requirements of the Act, 7–9
 - sections
 - 302 Corporate Responsibility for Financial Reports, 17–21, 168, 183–184
 - 404 Management Assessment of Internal Controls, 22–23, 168, 185
 - 409 Real Time Issuer Disclosures, 24–26, 168, 187
 - title summaries, 4–7
 - 1. Public Company Accounting Oversight Board (PCAOB), 4
 - 2. auditor independence, 4
 - 3. corporate responsibility, 4–5
 - 4. enhanced financial disclosures, 5
 - 5. analyst conflicts of interest, 5
 - 6. commission resources and authority, 6
 - 7. studies and reports, 6
 - 8. corporate and criminal fraud accountability, 6
 - 9. white-collar crime penalty enhancements, 6
 - 10. corporate tax returns, 6
 - 11. corporate fraud accountability, 7
- Securities Acts of 1933 and 1934, 4
- Securities and Exchange Commission (SEC), 3, 21
- Securities Exchange Act of 1934, 4, 9, 17,
 - 22
- Segregation of duties, 197–201
- Significant account, 47
- Significant deficiency, 44–45
- Significant process, 48–49
- Software applications, 133–136
- Solvency II, 177–180
- Standards for the Professional Practice of Internal Auditing*, 241
- Statement on Auditing Standards (SAS) No. 70, Service Organizations,
 - 126–130
 - type I and type II reports, 127
- Studies and reports (Title 7), 6
- Supplemental narratives, 202

Index

Technology, using, 151–153

Training plan for employees, 59

Tyco, 3

Unnecessary burden approach, 146

Users of financial data, 12–13

White-Collar Crime Penalty Enhancement
Act of 2002, 6

White-collar crime penalty enhancements
(Title 9), 6

WorldCom, 3, 12, 146