Sarbanes-Oxley
Internal Controls

Effective Auditing with AS5, CobiT,
and ITIL

ROBERT R. MOELLER
Sarbanes-Oxley Internal Controls

Effective Auditing with AS5, CobiT, and ITIL

ROBERT R. MOELLER

John Wiley & Sons, Inc.
Dedicated to my best friend and wife, Lois Moeller. Lois is my companion and partner whether we are on our Lake Michigan sailboat, skiing in Utah, traveling to all sorts of interesting places in the world, gardening in the backyard and cooking the results, or doing all sorts of home projects.
## Contents

### Preface

xi

### CHAPTER 1

**Introduction: Sarbanes-Oxley and Establishing Effective Internal Controls**

1

- Changes Since SOx Was First Introduced 3
- Converging Trends: ITIL, CobiT, and Others 7

### CHAPTER 2

**Sarbanes-Oxley Act Today: Changing Perspectives**

13

- Sarbanes-Oxley Act: Key Elements 14
- Impact of the Sarbanes-Oxley Act 51

### CHAPTER 3

**AS5 Standards for Auditing Internal Controls**

53

- AS5 Objectives 54
- Reviewing Section 404 Internal Controls Under AS5:
  - Introduction 57
- Planning the SOx AS5 Audit 59
- AS5's Top-Down Approach 66
- Testing Internal Controls 72
- Evaluating Identified Audit Deficiencies 75
- Wrapping Up the AS5 Audit 76
- Reporting on AS5 Audit Internal Controls 78
- Improving Internal Controls Using AS5 Guidance 79
- Going Forward: Potential Risks and Rewards 80

### CHAPTER 4

**Establishing Internal Controls Through COSO**

83

- Importance of Effective Internal Controls 84
- Internal Control Standards: Background 86
Events Leading to the Treadway Commission | 90  
COSO Internal Control Framework | 94  
Other Dimensions of the COSO Internal Control Framework | 116  

CHAPTER 5  
Using CobiT Framework to Improve SOx Controls and Governance | 119  
CobiT Framework | 122  
Using CobiT to Assess Internal Controls | 127  
CobiT and Sarbanes-Oxley | 141  

CHAPTER 6  
Performing Section 404 Reviews Under AS5: An Ongoing Process | 149  
SOx Section 404 Assessments of Internal Controls Today | 150  
SOx Section 404 Requirements | 152  
Section 404 Filing Rules: Changing Deadlines for Eligibility | 168  
Gaps and Compliance Committees Under Today’s SOx Rules | 173  
Documenting Internal Controls Going Forward | 178  
Control Objectives and Risks Under Section 404 | 180  

CHAPTER 7  
Other SOx Requirements: Sections 302, 409, and Others | 183  
Other Important SOx Compliance Rules | 184  
Section 302: Management’s Financial Report Responsibilities | 184  
Section 401: Off-Balance Sheet Disclosures | 188  
Section 409: Disclosures on Financial Conditions and Operations | 190  
Section 802: Penalties for Altering Documents | 192  
Section 806: Whistleblower Provisions | 193  
Keeping SOx Rules in Focus | 201  

CHAPTER 8  
Using ITIL to Align IT with Business Processes | 203  
Importance of the Information Technology Infrastructure | 204  
ITIL Framework | 206  
ITIL Service Delivery Best Practices | 208  
ITIL Service Support Best Practices | 221  
Security Management | 237  
Linking ITIL with CobiT and SOx Internal Controls | 239
The passage of the Sarbanes-Oxley Act (SOx) in 2002 almost seems like distant history today. That legislation became effective after a series of accounting scandals led to the failure of several then major corporations, such as Enron and WorldCom, the conviction and imprisonment of multiple key executives, and the failure of the major public accounting firm, Arthur Andersen. With a time-based registration schedule to become SOx compliant, enterprises worldwide have struggled to change their processes to become compliant with all aspects of these new SOx procedures, and there certainly have been many “bumps” on that road along the way.

Perhaps the largest impediment to SOx compliance was that many enterprises initially struggled with the new internal control documentation requirements and the auditing standards rules published by the newly established Public Company Accounting Oversight Board (PCAOB) regulator. Enterprise management and their internal auditors often did not have consistent and well-recognized approaches for reviewing and understanding internal accounting controls and for complying with their external auditor’s attest requirements. As SOx compliance was being rolled out to a wider group of enterprises both at smaller entities in the United States and others worldwide, there has been a recognized need for some changes surrounding SOx compliance.

The overall objective of this book is to describe and discuss some of the changes to SOx-related rules and supporting procedures since the legislation became U.S. law in 2002. Although there have not been any formal revisions to the basic SOx legislation at present, complying with SOx means following the rules established by the PCAOB and the SEC. A major objective of this book is to take another look at the more important aspects of SOx and to consider some of the changes and evolving standards that may make compliance easier for auditors and enterprise management.

This book will highlight some of the important or evolving new changes or frameworks that will make compliance with SOx less difficult for all enterprises, whether a domestic or a non-U.S. registrant. These same changes
are more control risk based and applicable to all enterprises, despite their relative size. This text will look at the current status of SOx from the perspectives of internal audit, IT, and enterprise management:

- **Chapter 1, Introduction: Sarbanes-Oxley and Establishing Effective Internal Controls.** We set the stage for the background and objectives of this book.
- **Chapter 2, Sarbanes-Oxley Act Today: Changing Perspectives.** While the basic SOx legislation has never changed, the SEC and PCAOB rules surrounding it have changed, and the emphases on some aspects of SOx have been mixed. This chapter will provide a high-level overview of the Act, emphasizing areas where compliance practices are changing, such as for Section 404 internal control reviews. In other instances, the legislation remains on the books, and there has been minimal attention given to some rules. For example, many predicted considerable activity surrounding the whistleblower rules in SOx. That just has not happened, and we will review the current status of these rules. In general, this chapter will look at the rules and caution signs that are important in SOx today for all levels of management as well as for internal audit. The chapter will focus on areas that an internal auditor should consider when reviewing the adequacy of SOx-related internal control procedures in place.
- **Chapter 3, AS5 Standards for Auditing Internal Controls.** This chapter will provide an overview of PCAOB auditing standards, with an emphasis on the newly issued and very important AS5 on auditing internal controls. These risk-based standards primarily apply to the manner in which external auditors perform their reviews, and each of the major public accounting firms has developed its own standards and interpretations of AS5 rules. This chapter will not attempt to critique public accounting audit procedures, but will outline the key elements of these standards that are important for managers and internal auditors in an enterprise.
- **Chapter 4, Establishing Internal Controls Through COSO.** The COSO framework for organizing and understanding internal controls in all aspects of an enterprise has become the de facto standard in the United States as well as, to a growing extent, worldwide. While the COSO internal control framework has been available for many years, this chapter will look at COSO from the perspective of establishing effective internal controls in a SOx environment, and will also include guidance to help review the adequacy of COSO internal controls.
- **Chapter 5, Using CobiT Framework to Improve SOx Controls and Governance.** As introduced in previous chapters, the CobiT framework
is a useful tool for organizing and assessing both business and IT internal control processes. This chapter will provide a fairly detailed overview of the most recent version 4.1 release of CobiT and outline approaches for using CobiT to better manage internal controls under SOx. This chapter will also link CobiT with the ITIL framework introduced in Chapter 8. Although CobiT was originally developed just for IT auditors, the chapter will focus on CobiT as a tool and standard for establishing Enterprise-wide SOx compliance.

Chapter 6, Performing Section 404 Reviews Under AS5: An Ongoing Process. Most larger, U.S.-based enterprises have now gone through several annual cycles of Section 404 reviews, with varying levels of frustration and pain. This chapter will discuss how to establish self-assessment processes and internal control improvement programs to help provide more value in SOx Section 404 processes. For the smaller-capitalization enterprises that are just beginning to become SOx compliant, this chapter will look at the risk-based changes to these rules to lessen burdens. For registrant enterprises, Section 404 rules can be tedious, but SEC and PCAOB changes have made this process less onerous. The goal should be to try to achieve process improvements through this SOx compliance work.

Chapter 7, Other SOx Requirements: Sections 302, 409, and Others. Many business managers think of SOx only in terms of its Section 404 internal control requirements. This chapter discusses several other areas of SOx that are important to both managers and auditors today, with an emphasis on Section 302, where management is responsible for signing off on reported results, as well as a series of requirements for audit committees. In addition, we will consider the implications of Section 409R that are pushing management to move to almost real-time reporting of financial results—the continuous close. We are not there yet, but the requirement may soon have major implications for financial and IT managers and their processes.

Chapter 8, Using ITIL to Align IT with Business Processes. The introductory paragraphs of this chapter talk about the growing recognition and importance of the ITIL set of best practices. This chapter will provide a complete overview of the ITIL service support and service delivery frameworks. The emphasis will be on the newly released version 3 of ITIL and how these best practice guidelines can be tied to CobiT when establishing effective SOx internal control processes. In particular, we will consider how compliance with ITIL best practices can change control processes and how these can be better built into improved management and internal audit processes.