SOX Illustrated:
An Easy-To-Understand Guide to the Sarbanes-Oxley Act

Bill Douglas
President
Cost Advisors, Inc.
# Table of Contents

## Acknowledgements

**Introduction** .................................................................................................................. ii

### About the SOX Illustrated Book ....................................................................................... ii

**Chapter 1:** A Review of Sarbanes-Oxley Rules from the SEC, COSO, and PCAOB .......... 1

- Part 1: A Review of the Sarbanes-Oxley Act .................................................................. 1
- Part 2: SEC vs. PCAOB .................................................................................................. 13
- Part 3: COSO .................................................................................................................. 16
- Part 4: Gaps and Deficiencies .......................................................................................... 22

**Chapter 2:** Project Scope, Schedule & Resources ............................................................ 40

- Part 1: Documentation & Testing ................................................................................... 40
- Part 2: Project Guiding Principles ................................................................................... 43
- Part 3: Project Organization ............................................................................................ 45
- Part 4: Project Team Staff .............................................................................................. 46
- Part 5: Materiality ............................................................................................................ 50
- Part 6: Documentation and Testing – Processes vs. Risks ............................................. 54
- Part 7: Hierarchy ............................................................................................................. 58
- Part 8: Project Size ........................................................................................................... 61
- Part 9: Account Risk and Assertions .............................................................................. 66
- Part 10: Process to GL Map ........................................................................................... 70
- Part 11: Project Timeline ............................................................................................... 71

**Chapter 3:** Analysis of Risks and Controls ....................................................................... 76

- Part 1: Wedding Cake-Entity Level Controls ................................................................. 76
- Part 2: Business Process Flowcharts .............................................................................. 84
- Part 3: The Risk and Control Matrix – Assertions ......................................................... 86
- Part 4: Controls ............................................................................................................... 90
- Part 5: Creating an Expenditures Risk & Control Matrix ............................................... 96

**Chapter 4:** Writing and Implementing Test Plans ............................................................... 101

- Part 1: Inherent Process Risk and Risk of Control Failure ........................................... 101
- Part 2: A Risk Based Approach to Testing .................................................................... 107
- Part 3: A Risk Based Approach to Testing II – External Auditor Reliance ..................... 114
- Part 4: A Risk Based Approach to Testing II – Compiling Work Papers ....................... 119
- Part 5: A Risk Based Approach to Testing III – A Test Plan Example ........................... 124
- Part 6: A Risk Based Approach to Testing III – Using A Random Number Generator ... 135
- Part 7: A Risk Based Approach to Testing III – Test Exceptions ................................... 138
Chapter 5: Documenting & Testing IT General Controls.......................................................... 143
  Part 1: IT Evaluation Frameworks ..................................................................................... 143
  Part 2: Testing IT General Controls .................................................................................. 149
  Part 3: Segregation of Duties Testing ............................................................................. 153

Chapter 6: Excel, Access, and Web-Based Applications...................................................... 154
  Part 1: Spreadsheet Controls ......................................................................................... 158
  Part 2: Choosing Useful Software Applications .............................................................. 162

Chapter 7: Summary of Sarbanes-Oxley 404 Best Practices........................................... 166

Appendix A: List of Processes .......................................................................................... 170

Appendix B: Sample Flowchart for Expenditure Cycle .................................................... 176

Appendix C: Risk Evaluation Spreadsheet ...................................................................... 178

Appendix D: Sample Test Plan for Expenditure Cycle ...................................................... 180

Appendix E: Deficiency Evaluation Form ......................................................................... 185

Glossary: Important Terms and Acronyms ..................................................................... 187
Acknowledgements

I’d like to thank everyone at Cost Advisors who contributed to the completion of this book. It was because of their hard work and dedication that this book was created.

- Sophia Ng – proofreading and project management
- Kristi Martin – proofreading
- Brian Call – proofreading
- Jackie Mawdsley – proofreading
- Daniel Prapailong – editing illustrations, glossary, and formatting table of contents
- Irene Yankelevich – editing illustrations and formatting
- Cost Advisors team – selecting the name
Introduction

About the SOX Illustrated Book
Introduction

SOX Illustrated

Bill Douglas, Principal Advisor
Cost Advisors, Inc.

About Cost Advisors and the SOX Illustrated book:

In 1999, Bill Douglas formed Cost Advisors in March 1999 to assist companies with financial-projects. Cost Advisors originally helped companies grow their bottom-line by showing them how to run more efficiently. Since inception, Cost Advisors consultants have successfully completed over three dozen projects of various types.

With the passage of the Sarbanes-Oxley Act, Cost Advisors clients asked for help with their Sarbanes-Oxley compliance projects. Since April 2003, Cost Advisors has been performing Sarbanes-Oxley work exclusively, including work for some of the most prominent companies in the Greater-Portland area. Cost Advisors, Inc. has also developed a free software application called SarbOxPro®, to assist companies with their Sarbanes-Oxley projects. The software can be downloaded at http://www.sarboxpro.com, and Cost Advisors has consulted with SarbOxPro customers nationwide.

Bill Douglas started Cost Advisors, Inc. with a broad background in financial consulting. Bill is a Certified Public Accountant (CPA) in Oregon and Pennsylvania, with practice privileges in Washington and California as well. He is also a Certified Internal Auditor (CIA) and a Certified Fraud Examiner (CFE). In addition to his background in accounting and auditing, Bill also brings a wide knowledge of IT systems to Cost Advisors, Inc. He is a Microsoft Great Plains Certified Installation Specialist, Certified Accounting Applications Specialist, and Partner. Bill's combined management experience in accounting, IT systems, sales, and marketing underlie the material in presented here.

This book came about because, aside from winning the lottery, there is no way to avoid Sarbanes-Oxley. While unavoidable, Sarbanes-Oxley is simple to understand. Cost Advisors, Inc. has a good conception of what works and what does not work because the company has been exclusively doing Sarbanes-Oxley work since the passing of the Act.
How to Use This Book

Before getting started, the reader should note some important keys to using this book. The red star (see the image above) indicates a “best practice.” The graphics that include a best practice will have this star on them. Best Practices are important because they save time and money in the Sarbanes-Oxley process.

This book relies on real-life case studies that have been adapted from Cost Advisors, Inc.’s vast SOX experience. The book follows various case studies through the Sarbanes-Oxley process, from planning to documentation, testing, and testing exceptions.

Because the Sarbanes-Oxley compliance process involves many different members of the project team, and participants both inside and outside the public company under review, this book will use the word “auditor” to refer to the individual conducting the audit. The auditor may in some cases be an employee of the company, and an external consultant in others. As they come up in the text, the book will note the specific functions for which the Sarbanes-Oxley Act requires the services of an external auditor.

Additionally, this book will use the abstract pronoun “he” to indicate a generic auditor. This in no way implies a corresponding gender for the auditor, but rather reflects prevailing grammatical standards. The key to effective Sarbanes-Oxley compliance is selecting a highly qualified project team. Whether team members are consultants or employees, their credentials and experience should override gender.

The Cost Advisors, Inc. Commitment

Cost Advisors, Inc. is committed to helping companies and consultants comply with Sarbanes-Oxley. Toward that goal, this book includes a 100% collective effort. Upon finishing this manual, the reader will know how to run a Sarbanes-Oxley project and have a little fun along the way. It only takes a bit of the reader's participation in the materials.

The goal of the book is to help readers save time in their SOX compliance efforts by planning, organizing and executing their SOX compliance in the most efficient way possible. Doing SOX properly can prevent companies from larger problems, such as misstatements and restatements, and even in preventing fraud. Companies can also get reliance from their external auditor and reduce their external audit fees.
Overview of the Book

Chapter one starts by reviewing the origins of the Sarbanes-Oxley Act (also called SOX for short) and the context of its passage through Congress. Next, the chapter explores the important Sarbanes-Oxley rules defined by the Securities & Exchange Commission (SEC), the Committee of Sponsoring Organizations of the Treadway Commission (COSO), and the Public Company Auditing Oversight Board (PCAOB). This review outlines each governing body and its role within SOX. Chapter one concludes by explaining deficiencies, which the Sarbanes-Oxley Act was designed to minimize as a means of restoring investor confidence.

Having reviewed the rules established by the SEC, COSO and PCAOB for Sarbanes-Oxley projects in chapter one, chapter two focuses on Scope, Schedule, and Resources. In short, the reader will learn how to determine the elements to include in a Sarbanes-Oxley project. Project planning is an essential first step to successful completion of an audit.

Chapter three examines risk analysis and controls. Part one of chapter three examines in greater depth the best techniques for analyzing risks and controls within business processes. The chapter begins with a detailed look at entity-level controls. This is followed by a description of how to develop flowcharts of business processes. Then the chapter will look at a case study and build a sample flowchart.

Part two of chapter three will focus on risk and control matrices and assertions. Starting from assertions, the reader will learn the method for developing a risk and control matrix as a means of accurately identifying all the relevant risks and appropriate controls. Next, part two will examine the importance of company level controls in relation to the risk and control matrix. Then this section will explore techniques for identifying the best controls. Finally, the chapter will conclude by developing a risk and control matrix for the ongoing case study of the expenditures cycle.

Chapter four focuses on writing and implementing test plans. The discussion begins with an analysis of the difference between risks inherent in business processes and the risk of control failure. This analysis is followed by an explanation of the heat sheet, a graphical method for representing requirements for testing based upon these risks. The second half of the chapter examines a risk based approach to testing. This section covers determining risk factors for both inherent process risks and risks of control failure through a rigorous, methodical method documented through the use of a spreadsheet. Finally, the chapter summarizes the risk-based approach, describing the judgments the auditor must make concerning testing standards within the framework of the given company's processes and controls.

Chapter five examines three approaches to evaluating the IT infrastructure or IT General Controls (ITGC). The chapter begins with a short review of the standards that have been developed for IT infrastructure. It continues with an outline of the most important IT controls. Lastly, the chapter finishes with a technique for analyzing segregation of duties problems in relation to IT systems.

Chapter six explains differences between various software tools that can help the auditor conduct a Sarbanes-Oxley project.

The final chapter summarizes the major concepts covered in the book.
Chapter 1:
A Review of Sarbanes-Oxley Rules from the SEC, COSO, and PCAOB

Part 1: A Review of the Sarbanes-Oxley Act
Who Wrote Sarbanes-Oxley?

The pictures above show Senator Paul S. Sarbanes of Maryland (ret.) and Congressman Michael G. Oxley of Ohio (ret.), the namesakes of the Sarbanes-Oxley Act. Both finished their terms in 2006. Interestingly, the two writers of Sarbanes-Oxley are not accountants but lawyers.

When Senator Sarbanes and Representative Oxley retired, many in the business world speculated that Congress would water down the Act as soon as its authors left office. Some people also thought that small companies might be granted an exemption from complying. None of this speculation came to pass, and in fact, Democrats, now in control of Congress, will probably not make changes that would weaken the Act. Now, many additional companies and non-profit organizations are applying a risk-based approach and control mechanisms. Application of a risk-based approach is not called Sarbanes-Oxley, but Sarbanes-Oxley started this trend.
Leading up to Sarbanes-Oxley

In the wake of financial scandals in 1999 through 2001, most notable, Enron, MCI WorldCom, HealthSouth, Adelphia, and Tyco, the US government took action to improve corporate accountability and governance. This took the form of Sarbanes-Oxley Act of 2002. However, the majority of government prosecutions for wrongdoing, related to the pre-SOX financial scandals listed above occurred under the existing securities laws prior to the Sarbanes-Oxley Act.

The chart above shows a perspective of what happened in the stock market that led to the passage of the Sarbanes-Oxley Act. The chart plots the Dow Jones Industrial Average from 1957 to 2006 and indicates a clear fall off in the market between 1999 and 2002. While irrational exuberance and overpriced stocks caused some of this dip in the market, low investor confidence led to a good portion of it. Not a lack of confidence in a few companies, this was a general lack of confidence in the market as a whole. The overarching goal of the Sarbanes-Oxley Act was to restore investor confidence in the market.

Many people wonder if Sarbanes-Oxley was an overreaction. Other critics speculate as to whether or not the Act will prevent the same situation from developing again. It is impossible to know whether Sarbanes-Oxley was an overreaction or if it will prevent future losses of confidence. However, the Act did accomplish the goal of restoring investor confidence. The Sarbanes-Oxley Act did pull the market out of a trough and head it toward new record highs.

A close look at this graph shows that the Sarbanes-Oxley Act was passed near the bottom of the market fall-off caused by lack of investor confidence. Just after that, the SEC published its Sarbanes-Oxley rules, and investors started to regain confidence. The newfound sense of confidence in turn led to a new rise in the market. Not all of the credit can be given to the Sarbanes-Oxley Act, but it did have an important influence.
The median loss due to fraud for all U.S. companies, both publicly traded and private, was $159,000 in 2006. One fourth of these cases caused at least $1 million in losses for the company. U.S. organizations lose approximately 5% of annual revenues due to fraudulent activity. This number is validated every 2 years by the Association of Certified Fraud Examiners. The ACFE takes a poll of about 1,000 fraud examiners and the cases they work with to determine this estimate. If you were to multiply the 5% by the U.S. gross domestic product you would come up with $652 Billion lost to fraud. Most occupational fraud schemes involved either the accounting department or upper management. Fraud involving upper management tends to produce larger losses. This estimate is only based on the reported cases of fraud, most companies keep fraudulent activity quiet because they do not want the negative publicity. The percentages in the graph above do not equal to 100% because most cases of fraud involve more than one of the three categories.
The number of companies restating financial results rose sharply in the wake of the Sarbanes-Oxley Act. 2004 was the first year companies were required to comply and in 2005 the number of restatements rose sharply. There are 10,000-11,000 public companies in the U.S. and 1,800 had restatements (18%) in 2006. Only half of these companies are accelerated filers and required to have an external audit for SOX. The other half, the non-accelerated filers, is required to do an internal audit for their SOX projects. In 2009 these non-accelerated filers are required to be externally audited for SOX compliance. It is expected that the number of restatements will increase again due to these small companies.
The Sarbanes-Oxley Act of 2002

Here is the Sarbanes-Oxley Act of 2002. At least, that is its short title. For ease of discussion, this book will abbreviate the title to the Sarbanes-Oxley Act, Sarbanes-Oxley, SOX, or the Act.

One Hundred Seventh Congress
of the
United States of America

AT THE SECOND SESSION
Began and held at the City of Washington on Wednesday,
the twenty-third day of January, two thousand and two

An Act
To protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS
(a) SHORT TITLE.—This Act may be cited as the “Sarbanes-Oxley Act of 2002”.

6
The PCAOB

Although Sarbanes-Oxley is not complicated, it does require knowledge of an entirely new vocabulary. The first term is PCAOB; everyone who works with SOX pronounces it "peek-a-boo," but it is the acronym for the Public Company Accounting Oversight Board. The PCAOB is a five-member organization formed out of the Sarbanes-Oxley Act. On an interesting note, only two of the members can have been public accountants. At the time the Act was passed, legislators had a strong desire to limit the influence of the accounting profession.

Sarbanes-Oxley requires auditors of existing public companies to register with the PCAOB. Auditors have 180 days to register so that the PCAOB can in turn review them. Once an auditor performs an audit, the PCAOB is authorized to examine that auditor's work. The PCAOB process established review system for auditors; however, unlike other peer review systems, the PCAOB publishes its findings on the PCAOB website.
Importantly, the PCAOB also conducts annual reviews of auditing firms that perform more than 100 audits of public companies in a year. The PCAOB conducts reviews every three years for firms performing fewer than 100 audits of public companies each year. This list of links to the PCAOB inspection reports of individual audit firms can be found on the PCAOB website.

Public companies pay for PCAOB reviews through a tax; auditors (currently large accounting firms) do not. This tax, based upon market capitalization of the public companies, covers the major part of the PCAOB’s $144 million budget. Auditors only pay a registration fee that covers the cost of processing their application (to be external auditors of public companies) totaling $40,000, only a very small portion of the budget. The remainder of the budget ($134 M) is funded by public companies. The PCAOB “tax” calculation on public companies is as follows:

\[
\text{PCAOB Annual Budget} \times \frac{\text{Public Company Market Capitalization}}{\text{Total Market Capitalization (1)}} = \text{PCAOB "Tax"}
\]

(1) US Companies with Market Capitalization > $25M

Despite receiving partial funding through a tax on public companies, the PCAOB is not a governmental entity; it is a non-profit organization. The PCAOB reports to the SEC but is not funded by revenue from individual taxpayers. As such, PCAOB operations are supported by the public companies it oversees, keeping it separate from the government. However, while the PCAOB is not a government entity, it must have SEC approval before publishing any findings.

Public Company Records

One of the most important aspects of SOX compliance is that companies must keep their own records concerning their internal control structure. For example, if a company had fraud that was properly recorded – someone debited expense and credited cash, and it was material fraud, it would be a problem under the Act. The mere fact of fraud, even with properly recorded transactions and correct financial statements, indicates an internal control weakness, and SOX considers this a problem.

External auditors often bring up this type of properly recorded fraud in discussions about the scope of Sarbanes-Oxley. Controls that ensure correct financial statements are well within the scope of the Act. Companies must record receipts and expenditures according to management's authorization. If someone commits fraud or even if they make a purchase for the company without having the authority to make that purchase, an internal control problem exists according to SOX. For example, a company has an internal control problem if somebody in IT buys a big mainframe without the board or top management delegating the authority for that purchase to the IT department.

Although examples like this one might seem beyond the scope of Sarbanes-Oxley, they actually fall within its purview. The Act requires consideration of management's authorization for each action taken on behalf of the company, even when financial statements are correct.

Auditor Independence

Sarbanes-Oxley also established new rules for keeping auditors independent from the public companies they are reviewing. For example, one of the big problems with the Enron scandal was that Enron was paying Arthur Andersen about $50 million a year for consulting and about $18 million a year for the audit. Although
Chapter 1 – SEC, COSO, & PCAOB Rules

Arthur Andersen was acquitted, a conflict of interest was highly possible since they were earning more for consulting than for auditing. This arrangement might create the perception that Arthur Andersen would not want to jeopardize its $50 million consulting fee because of a damaging audit. In order to avoid such conflicts of interest, public accounting firms are no longer permitted to perform tasks that conflict with external audit services. Auditors can no longer do bookkeeping, they cannot keep any records, and they cannot design or set up financial information systems for the client. These rule changes are important because around 1999-2000, accounting firms viewed audits as a commodity. That is to say, firms used audits to develop relationships with clients in order to get IT systems or consulting contracts. Under Sarbanes-Oxley, firms can no longer use audits in this manner.

Auditors are forbidden from performing other functions for their clients as well. Auditors cannot do appraisals, valuations, or actuarial work. They can no longer do the internal audit and the external audit; they cannot be a broker-dealer; they cannot carry out human resources or other management functions; and they cannot perform legal services.

Accounting firms may still provide some tax services for the clients they audit. One additional loophole also exists: auditors can perform some functions if the company's Board of Directors approves them. In terms of compliance, it is very important to ensure that auditors are not performing any of the prohibited services for companies they are auditing, and if they are offering other services, like tax advice, that they have the PCAOB's approval to do so.

Audit Partner Rotation

In addition to keeping a separation between accounting firms and consulting tasks performed for public companies, Sarbanes-Oxley also requires that audit partners rotate every five years. Furthermore, auditors must wait at least one year after the audit before going to work for clients as CEO, CFO, Controller, or Chief Accounting Officer.

Audit Committees

The passage of the Sarbanes-Oxley Act also caused a rush to find financial experts because it required the presence of at least one CPA or financial expert on the audit committee of the Board of Directors of each public company. Only about 20,000 people participate on Boards of Directors, and some of these people sit on as many as 10 boards. However, very few board members are CPAs or financial experts. As a result, the Act led to a scramble, not only to set up audit committees on Boards that did not have them, but also to find financial experts, who are still in short supply among board members.

Section 302 – the Heart of Sarbanes-Oxley

Section 302 deals with the quarterly compliance measures in Sarbanes-Oxley as well as with changes of internal control. At its root, section 302 requires companies to disclose any changes they have made to their internal control structure. Even positive changes to internal controls must be reported, although companies usually do not do so.

While section 302 is very similar to section 404, the main point the reader should take from 302 is that company executives are required to note any changes to internal controls and any new monitoring mechanisms put in place to ensure the proper function of those controls. Executives must note new controls and monitoring mechanisms in every financial report (10-Q and 10-K).
Most public companies were not prepared for quarterly certification of changes. This testing process is expensive, and some companies limit costs by targeting only the highest risk controls for testing every quarter or every other quarter. These companies then supplement the limited testing with confirmation reports from department managers such as the head of payroll, the head of A/P, the head of order entry, and the fixed asset manager who attest that there are no weaknesses or changes in controls. Having these confirmation reports provides greater security for the CFO and CEO who must sign off on Section 302 each quarter.

Those who work closely with SOX call these department managers process owners. “Process owner” is another important term to learn. For example, instead of saying, “The AP manager is the department manager of accounts payable,” one would say, “The AP manager is a process owner.” These sentences mean the same thing; the process owner manages a department in which financial activities and controls occur.

Additionally, accounting firms auditing public companies must keep their work papers for five years after the audit, and the public companies themselves are required to keep their SOX compliance materials for seven years. This regulation was included in the Act to prevent situations like the Enron scandal where all of the audit materials were shredded shortly after completion of the audit. Requiring the storage of work papers also has important implications for IT; for example, email systems need backed up and the tapes kept for 5 years.

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.

Also, officers and executives can no longer borrow money from the company. This rule was implemented to prevent future abuse of what had been a rash of “officer loans” being forgiven.
These 167 words created all the work mandated by Sarbanes-Oxley. As mentioned above, the goal of the Act was to restore investor confidence. Before SOX, CEOs and CFOs were placing the blame for financial reporting problems on their subordinates. SOX requires that the CEO and CFO accept responsibility and not attempt to place it on the controller, accounting manager or any other employee. This acceptance of responsibility is not only a matter of signing off on the reports, but also requires documenting the controls and testing them too. Ensuring that the company has documented and tested all controls to verify that they function properly is the essence of Section 404.

Financial Experts

The Sarbanes-Oxley Act refers quite often to “financial experts.” A financial expert is someone who, through either education or experience, has an understanding of generally accepted accounting principles (GAAP) and financial statements. Experience may include public accounting or auditing (the Act does not specify CPA), or working as a principal financial officer or controller of an issuer (i.e. a public company). Financial experts are also required to have experience preparing or auditing financial statements of public companies that are similar to their own company. Finally, financial experts are required to apply accounting principles for estimates, reserves, accruals, and all typical procedures performed by a controller, accounting
Chapter 1 – SEC, COSO, & PCAOB Rules

Manager, or CFO. Within these procedures, the financial expert must also have experience with internal controls and understand audit committee functions.

Penalties

Any CEO or CFO who signs off on reports that do not comply with SOX requirements is subject to a fine of $5 million and a 20-year prison sentence. To date, however, no one has received the maximum penalty. Some of those charged have been acquitted. One clear example of such an acquittal is the case of Richard M. Scrushy of HealthSouth Corporation. HealthSouth is a rehab hospital chain that allegedly overstated its earnings in its effort to beat analysts’ estimates. Scrushy had signed an attestation of responsibility, but was acquitted by a jury, avoiding the $5 million fine and 20 years in jail.
Chapter 1:  
A Review of Sarbanes-Oxley Rules from the SEC, COSO, and PCAOB

Part 2: SEC vs. PCAOB
SEC vs. PCAOB

PCAOB and Auditing Standards

Another important term that comes out of Sarbanes-Oxley is the Auditing Standard (AS). The AS is the main PCAOB document that regulates the accounting firms auditing public companies. Auditors pay close attention to these statements published by the PCAOB. In fact, some try to predict the PCAOB's next pronouncement. Following these pronouncements is the way auditors keep up with the PCAOB's recommendations. The original SOX pronouncement was AS No. 2, and the most current pronouncement as of this printing, is AS No. 5, published in May 2007.

The SEC sets regulations for public companies, as it always has. The PCAOB was formed to review external auditors, not public companies; this would simply duplicate the role of the SEC. However, when the PCAOB publishes a new Auditing Standard, the SEC publishes the same information for public companies. The PCAOB version is usually more detailed than the SEC version.

Public companies have taken to reading the PCAOB version of each new pronouncement first, since it will tell them about the information auditors will need. Reviewing the SEC version is a second step. Public companies now not only need to be aware of SEC information, but also of PCAOB Standards as well.
Small Public Companies and PCAOB Auditing Standards

Because of the effort and expense involved in compliance with Sarbanes-Oxley, many groups lobbied the SEC and the PCAOB for changes. Chief among these groups were small public companies, which devote a disproportionate amount of their profit to the review process in comparison to their larger peers.

AS No. 5 is not the first reduction to requirements for auditors. Those familiar with internal audits will understand the different types of evidence required for testing: inquiry, observation, corroboration, examination of evidence, or re-performance. Each of the five levels of evidence provides greater accuracy than the previous one. Some of the original PCAOB auditing standards approved of inquiry and observation as sufficient methods. However, public companies ran into conflicts if they were unable to provide evidence of inquiry or observation to external auditors. Auditors, new to the SOX process, were charging by the hour rather than by the project, and at the same time would not accept a lower testing standard because of the PCAOB oversight to which they are now subject. The culture surrounding SOX audits is changing slowly, but AS No. 5 attempts to clarify requirements regarding the top-down, risk-based approach, external auditor reliance, the definition of material deficiency and other matters.

Section 404 Scope

**Annual Report of effectiveness of ICFR**

- ick' if er
- ICFR= Internal Controls over Financial Reporting

**Scope:**
- Detailed, accurate records to reflect transactions and dispositions
- Transactions roll up to Financial Statements which comply with GAAP
- Management has authorized receipts and expenditures
- Prevent or Detect unauthorized acquisition, use or disposition – IF MATERIAL

**Internal Controls Over Financial Reporting (ICFR)**

The next important acronym coming out of SOX is ICFR; pronounced “ick’ if er,” ICFR stands for Internal Controls over Financial Reporting. ICFR covers important aspects of section 404. First, as mentioned above, public companies must keep their own records. Secondly, transactions must roll up to financial statements that comply with GAAP. Thirdly, management must authorize all receipts and expenditures. As in the earlier example, even properly recorded fraud not authorized by management, must be noted as a deficiency under section 404.

Lastly, the company must also protect its assets. As in the example used earlier, a company acquiring or disposing of assets must protect them. Hard assets such as inventory must be kept locked up; hard assets that are not securely stored present control deficiencies.

These four aspects are important. Auditors working with SOX will demand more than just correct financial statements.
Chapter 1:
A Review of Sarbanes-Oxley Rules from the SEC, COSO, and PCAOB

Part 3: COSO
Yet another term important to Sarbanes-Oxley is the Committee of Sponsoring Organizations (COSO) cube. The diagram above shows the original COSO cube, developed in 1985 by the Treadway Commission; current versions of the cube include more concepts. The COSO cube seems complex, but in essence, it is composed of just five ideas. The first concept is the Control Environment. Located at the base of the cube, the Control Environment simply means that if the company is not honest and ethical, none of the rest of the cube matters. For the sake of simplicity, the Control Environment will be used synonymously with company level controls, entity level controls, and “tone at the top.” In sum, Control Environment assumes no lying, cheating, or stealing within the company, especially among executives.

The next level of the cube is Risk Assessment. Those who work with SOX speak about a “risk-based approach.” A risk-based approach means attempting to account for all potential problems. Proper technique for anticipating potential problems will be covered later in this book, but for now, the question to keep in mind is, “what are all the things that could go wrong?” The reader should note that not all potential problems concern financial statements; problems can occur with safeguarding assets or with management authorization.

The third layer of the COSO cube is Control Activities. Control Activities are the measures taken to ensure that anticipated problems do not occur. These Control Activities correspond to the issues raised during the Risk Assessment.

The relationship between the bottom three elements of the COSO cube is clear, but the next two layers often get left out. They are usually only dealt with in an indirect way. The fourth part of the COSO cube, Information and Communication, means understanding how information passes from person to person, and from department to department within a company. Specifically, it involves understanding how employees transmit information about problems. For example, if an employee finds that a bank account does not reconcile, examining information and communication requires identifying the people who are told about the problem and the information that gets passed along; in short the procedures for reporting and documenting issues. Just after Sarbanes-Oxley was passed, companies wrote out narratives to explain Information and
Communication procedures; however, using flowcharts offers a much better way to document information and communication processes (Chapter 3 describes flowchart development).

The final layer of the COSO cube is Monitoring. Monitoring requires devising means of testing control procedures to ensure that they actually work as planned. Mechanisms include internal auditors, the SOX procedures themselves, and IT system monitoring. While SOX does not deal directly with Information and Communication or Monitoring, these aspects are integrated into the Act.

The side of the COSO cube states that the considerations on the front of the cube must be applied to every process (units and activities) and location in the company. The auditor must consider parents, subsidiaries, sales offices, and stores – all of the units or operating units that have controls placed upon them and where financial reporting risks could occur. Chapter 2 covers the issue of scope, but the audit must not be restricted to the company headquarters.

The top of the COSO cube shows the areas it addresses. As mentioned above, COSO was started in 1985 when 12 accounting firms organized in response to corporate scandals in the late 1970s. They wrote an internal control standard as a way to structure thinking about audits. This standard, the COSO Cube, was designed to ensure that not only were financial statements correct, but also that operational controls complied with policies. Internal auditors today must still examine operational controls because non-compliance with policies can have serious financial implications due to lawsuits and fines. However, while COSO covers operations, financial reporting, and compliance with laws, SOX only deals with financial reporting (as well as management authorization and safeguarding assets).

Sarbanes-Oxley Section 404

**COSO Objectives** vs. **Section 404**

![Diagram showing COSO Objectives vs. Section 404 Scope]
Section 404 Scope

The diagram above shows the elements from the top of the COSO cube in a different format. Sometimes financial reporting does affect operations. Take for instance, inventory, which falls under financial reporting and operations. On the diagram, inventory would lie in the area at the intersection of the two respective circles, and thus within the scope of SOX. Other risks that might crop up under operations, such as building a product that no one wants to buy, do not fall under financial reporting and thus are beyond the scope of SOX.

On the other side of the diagram, there are laws that fall under financial reporting as well, such as the Securities Exchange Act. These laws would fall within the scope of SOX since they concern financial reporting. Other laws, concerning environmental protection or hiring for instance, do not influence financial reporting, and thus are outside the purview of SOX.

While the borders between what falls under financial reporting and what does not are murky, the auditor aims to deal only with those related areas of operations and regulations that fit squarely within financial reporting. The SOX project is large enough already that the public company cannot deal with the gray area at the fringes. The auditor's focus must be ensuring correct financial reporting, management authorization of transactions, and safeguarding assets. The reader should note that limiting the scope of an audit is essential to running an effective project.

COSO Small Business Guidance
COSO and Small Public Companies

Many small company officers have argued that SOX treats small public companies unfairly because they have smaller profits than their larger counterparts but just as many processes to document and test. The SEC responded to this argument by forming a Small Business Advisory Committee to study how SOX should be implemented for small public companies. At the end of a yearlong study, the Small Business Advisory Committee recommended that small companies be exempt from SOX. However, the SEC rejected this proposal, so for now, small public companies must still comply.

COSO, which devised the original internal controls adopted by public companies, published the Small Business Guidance manual, pictured above, in mid 2006. Small companies complying with SOX should buy a copy of this manual. The PDF version is available for download from http://www.cpa2biz.com and includes three PDF volumes and one MS Word template for SOX projects. The Small Business Guidance is a great guide with many practical suggestions. Because COSO set the original standards for internal controls, external auditors will usually accept these recommendations for limiting the scope of a project.
Sarbanes-Oxley Section 404

Overview

Summary: Internal Control

The pyramid shown above summarizes the material covered so far. Sarbanes-Oxley mandates that companies required to comply with the Act must choose an internal control standard. Probably 99% of all companies have chosen the COSO standard because it is the only standard in the United States. There is a Canadian standard called COCO (COCO is not a misspelling of COSO, it refers to the Canadian standard).
Chapter 1: A Review of Sarbanes-Oxley Rules from the SEC, COSO, and PCAOB

Part 4: Gaps and Deficiencies
Deficiencies, Significant Deficiencies and Material Weaknesses

As in a traditional audit, SOX audits are based on materiality. A traditional or substantive audit considers an amount on a balance sheet and tries to determine whether it is material. With SOX, the auditor examines the amount of materiality that flows through a process, not necessarily the balance in an account. The process, and its relationship to a chart of accounts, is most important here. The difference between a process and a general ledger account will be described below. The reader already undoubtedly knows what a trial balance and a chart of accounts are.

A process consists of job activities involving transactions that will ultimately be reported in the company's financial statements. Like water flowing in a stream, one can measure the annual volume of transactions involved in a given process. Taking payroll as an example, the SOX auditor can easily find out a company's annual payroll figure. The auditor then compares annual payroll with the materiality at the company (while payroll might not be material, that is an unlikely situation). There will however be some activities that are not material. For instance, company travel and entertainment expenses may not be high enough to be material. This is to say that materiality varies for each individual company. SOX auditors use the same standard for materiality as in a substantive audit, although this is not necessarily the same standard for materiality as in an internal audit.
The top of the diagram above contains three blocks (ignoring for a moment the part labeled control deficiency at the bottom). These blocks indicate the three levels of problem severity under SOX: deficiency, significant deficiency, and material weakness. Deficiencies fall into the green block at the left, significant deficiencies into the central yellow block, and material weaknesses into the blue block at the right. The difference in severity is based upon the dollar amount of the problem that has been discovered.

On a related note, those experienced with SOX refer to a significant deficiency as an “SD” and a material weakness as an “MW.”

If the auditor finds significant deficiencies (SDs), he must inform the audit committee. If the auditor finds material weaknesses (MWs), the company must notify shareholders as well. As a result, it is not a good practice to set a fixed line between SDs and MWs. A public company does not want to start a SOX project by stating an absolute materiality; rather the company should start with a judgment materiality. This gives the company some latitude to consider the circumstances surrounding the findings.

Because problems change from deficiency to SD to MW based upon the dollar amount involved, the bottom part of the chart becomes important. If a problem turns out to be material, but the likelihood of its occurrence is remote, it remains a deficiency. That is to say, if the dollar amount is large, but the probability is remote, the problem remains a deficiency.

New PCAOB Standard

New PCAOB Standard
Top Down approach Re-Emphasized
− Company level Controls can substitute for Process Level Control
− Look for Management Override
Risk-based approach re-emphasized
− Risk exists without misstatements
New Definitions of SD and MW
− ‘Reasonably Possible’ (less stringent than ‘More than Remote’)
− External Auditors shall not look for SDs (but still need to find control weaknesses that AGGREGATE to MW)
− SD = Significant, merits attention (less stringent than more than inconsequential)
− Weak Control Environment not automatically an SD (but still a strong indicator)
  ▪ Uncorrected SDs are a Control Environment issue
Materiality = same as the audit

The New PCAOB Standard

The new PCAOB standard brings in several new terms. The first is the Top-Down Approach. The Top-Down Approach requires starting from the Control Environment (see the COSO cube). While at the bottom of the COSO cube, this is called the Top-Down Approach, because it is a top-level control.
Chapter 1 – SEC, COSO, & PCAOB Rules

The second important term from the new standard is the Risk-Based Approach described earlier.

Existing definitions for significant deficiencies and material weaknesses have been changed. The old standard stated that a problem whose probability is “more than remote” falls into the category of significant deficiency or material weakness. The new standard changes that threshold to “reasonably possible,” the same definition used by FAS5. This change was made to keep consistency among existing practices.

Going back to the chart on the previous page, the threshold for significant deficiencies used to be “more than inconsequential,” but it has changed to “merits attention.” “More than inconsequential” did not emphasize the required communication (to the Audit Committee). The new standard focuses the auditor’s attention on the communication requirement. In general terms, if materiality is $1 million, then 20% of that, $200,000, is a significant deficiency. However, this changed in the new guidance, which states that a problem that “merits attention” is an SD and should be brought to the attention of the audit committee.

New PCAOB Standard

Streamlining PCAOB Procedures

The PCAOB has eliminated some unnecessary procedures; important among these is the evaluation of management assessments. Now auditors produce their own assessment, sometimes relying on work done by the client.

Also, under early versions of Sarbanes-Oxley, if a public company had subsidiaries, the audit had to encompass enough locations to cover 80% of revenue. This is not a great practice. The new guidelines require examining the risks at each individual subsidiary. The auditor should only include subsidiaries in the audit if they present a risk. Thus, rather than focusing on a fixed percentage of revenue, the audit should assess risks across the whole company.

As mentioned above, the auditor can now rely upon work that clients have done. The auditor no longer forms an opinion of the management's assessment, but he can incorporate it into his work. If he is going to rely upon management's assessment, however, the auditor must at least present his opinion of that assessment. Using work done by the client can offer huge savings of both time and money for the audit.
Public companies that complete a high quality internal assessment can set up an agreement with the auditor to rely upon the internal assessment even before work begins. The best practices for internal assessment will be covered later in this book, but essentially what is involved is having competent, objective, independent testers and performing the work according to accepted standards. The real savings comes when the external auditor can rely upon the internal assessment and avoid doing his own work. This will save on the number of hours that the auditor has to budget for the project. Cost Advisors, Inc. has seen this type of savings in many different engagements.

Conducting strong internal assessments also puts company executives at ease when they have to sign their approval of these assessments. The executives may also have a different set of objectives beyond materiality.

Different objectives (beyond materiality) may create a situation where the executives want a subsidiary that is clearly immaterial to be included in the assessment. While limiting the scope of the audit offers potential savings, if expanding the scope will make the executives feel more comfortable about signing off on the assessment, the auditor should go along with the management's decision.

### Non-Accelerated Filer vs. Small Company

<table>
<thead>
<tr>
<th>Category</th>
<th>Market Cap (# Sh x Stock Price)</th>
<th>Revenue Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Large Accelerated Filer</td>
<td>$700M</td>
<td>&lt; $250M Revenue</td>
</tr>
<tr>
<td>(10K in 60 days)</td>
<td></td>
<td>Small Public Company</td>
</tr>
<tr>
<td>(10Q in 40 days)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Accelerated Filer</td>
<td>$75M</td>
<td></td>
</tr>
<tr>
<td>(10K in 75 days)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(10Q in 40 days)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Non-Accelerated Filer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(10K in 90 days)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(10Q in 45 days)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Non-Accelerated Filers vs. Small Companies

The New PCAOB guidance makes an important distinction between accelerated and non-accelerated filers. The PCAOB now states that small companies can save money by doing things in a different way. On the left side of the chart, before Sarbanes-Oxley, there was a difference between accelerated filers, non-accelerated filers, and even large accelerated filers. This has all changed.

Non-accelerated filers have a market cap of $75 million or less. The market cap is simply the number of shares outstanding multiplied by the stock price as of June 30th. Non-accelerated filers had to comply with SOX for the first time in 2007. However, they only had to comply internally. The non-accelerated filers must have an external audit for SOX in 2009 (for fiscal years ending after December 15, 2009).

Accelerated filers, those companies with a market cap above $75 million have just completed their fourth filing in 2007. This is to say that they have now been complying with SOX for several years and have a good understanding of it.

The right side of the chart brings in the term “small company.” According to the PCAOB definition, a small company has revenue of $250 million or less and a market cap under $700 million. It is clear from these definitions that a small company is not equivalent to a non-accelerated filer; many more companies are classified as small than as non-accelerated filers.

New PCAOB Standard

<table>
<thead>
<tr>
<th>New PCAOB Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scaling audits for small companies</strong></td>
</tr>
<tr>
<td>Attributes of small companies:</td>
</tr>
<tr>
<td>− Few business lines</td>
</tr>
<tr>
<td>− Less complex business processes and financial reporting systems</td>
</tr>
<tr>
<td>− Centralized accounting functions</td>
</tr>
<tr>
<td>− Extensive involvement by senior management in the day-to-day activities of the business</td>
</tr>
<tr>
<td>− Few levels of management, each with a wide span of control</td>
</tr>
<tr>
<td>Testing:</td>
</tr>
<tr>
<td>− Inquiry &amp; Observation instead of documented evidence</td>
</tr>
<tr>
<td>− More reliance on Company-level controls</td>
</tr>
<tr>
<td>− Greater risk of management override</td>
</tr>
<tr>
<td>− Less SOD – test ‘alternative’ controls instead</td>
</tr>
<tr>
<td>− Greater competence risk</td>
</tr>
<tr>
<td>− Rely on IT packages application controls</td>
</tr>
<tr>
<td>− More new guidance in 2007</td>
</tr>
</tbody>
</table>
Auditing Small Companies: Company-Level Controls

The chart above lists additional criteria for defining a small company. Companies that fit this description can use inquiry and observation instead of documented evidence for some of their testing. Although the SEC and PCAOB both recommend using these types of evidence, auditors probably will not do so unless there are aspects of these methods that can be put into the work papers.

Among the new guidelines, greater reliance on company-level controls is probably the best area to save effort in an audit of a small company. While some company-level controls are concerned with ethics, most company-level controls are practices at the top of the company that would detect errors in a business process. Comparing budget to actual and investigating each variance greater than a certain percent or dollar amount is an example of a company-level control. The second step is writing up these findings along with the reason for the variance. Such a comparison can be an effective internal control and can prevent the need for detailed testing inside payroll and expenditures. Completing this kind of top-level review with enough sensitivity can thus eliminate a great deal of work. The savings from company-level controls is huge, if they are well done and documented, because they cut out detail work.

PCAOB Preliminary Guidance for Smaller Companies

AN AUDIT OF INTERNAL CONTROL THAT IS INTEGRATED WITH AN AUDIT OF FINANCIAL STATEMENTS:

GUIDANCE FOR AUDITORS OF SMALLER PUBLIC COMPANIES

October 17, 2007

The PCAOB guidance for smaller companies has been long awaited. Unfortunately, it was released by the PCAOB toward the end of the year that small public companies were supposed to comply with the preliminary guidance. As of the issuance date of this book, the PCAOB guidance for smaller public companies remains in draft form, awaiting approval by the SEC.
Purpose & Approach

**Purpose**
- Make the audit of internal control scalable for smaller, less complex companies
- Does not replace Auditing Standard#5

**Approach**
- Working group composed of auditors who have experience with smaller companies
- Consulted with financial executives from smaller public companies

The above chart outlines the purpose and approach that an auditor should take with a smaller public company when a smaller public company is trying to comply with SOX. In general, smaller public companies are less complex and the audit of internal control over financial reporting should be scalable. The proposed guidance was developed by the PCAOB by working with a number of auditors and financial executives from smaller public companies to provide the PCAOB feedback on the approach and execution of audits of internal control for smaller public companies.
5 Attributes of Small Companies

**Five Attributes of Small Companies**
- Fewer business lines
- Less complex business processes and financial reporting systems
- More centralized accounting functions
- Extensive involvement by senior management in the day-to-day activities of the business
- Fewer levels of management, each with a wide span of control

Previous definitions defined a small company as having a market cap of less than 700 million. Again, this is different than a non-accelerated filer, which is defined as having a market cap of just 75 million.

Small companies generally have fewer lines of business, less complex business processes, more centralized accounting functions, and extensive involvement with senior management and day to day activities. In other words, management of small companies can generally walk around the office and know what is going on. Further, small companies have fewer levels of management and the CFO generally knows all of the employees in the accounting department and many in the other departments. Employees in a small company usually do more and have a wider span of control than people in a larger company.

Scaling the Audit

**Scaling the Audit**

**Issues/Opportunities**
- More use of entity-level controls
- Risk of management override
- Limited opportunity to segregate incompatible duties
- Less complex (off-the-shelf) information systems
- Tougher to maintain financial reporting competencies
- Less formal documentation to run the business
- More deficiencies, ineffective entity-level controls

The above chart shows special audit considerations that small companies should watch for. Again, this is the proposed guidance that the PCAOB is giving to the external auditor. (COMMENT: this guidance is for everyone, not just the external auditor.)

In a small company, you can rely more heavily on entity-level controls. Entity-level controls are the top level controls that may save you time in performing controls documentation and testing at the business process level.

There is a greater risk; however, of management override at a small company, as a small company has a more limited opportunity to segregate duties due to its limited number of employees. Management can
override controls more easily as a result of the lack of proper segregation.

Further, the IT systems of small companies are usually less complex and less customized and it’s tougher for small companies to maintain financial reporting competencies because it’s tougher for small companies to hire the best people and to retain them. The documentation (not just SOX documentation, but all documentation) at a small company is generally not as formal as that of a large company. And usually in a small company, more deficiencies arise and entity-level controls are ineffective.

**Auditor Reliance on Controls**

The diagram illustrated above is true not only for a small company, but also for large companies. The diagram shows that stronger controls of a company can lead to heavier reliance on the financial statements. In other words, the auditor can perform fewer substantive tests if the auditor can place heavier reliance on controls. However, stronger controls do not necessarily mean that the financial statements are free of misstatements.

**Types of Entity-Level Controls**

- Control environment
- Management override
- Risk assessment process (SOX)
- Centralized processing including shared service environments
- Monitoring results of operations, other controls and audit committee and self-assessment programs
- Financial reporting process
The control environment, management override, risk assessment process, centralized processing, monitoring results of operations, financial reporting process and policies are types of entity-level controls.

The first type of entity-level control is the type of control that provides only an indirect effect on the overall control environment. The second type of entity level control is the type that monitors that another type of control is functioning properly. For example, if someone is performing a bank reconciliation, then the person performing the bank reconciliation is actually performing the control. Then when you have the CFO reviewing that bank reconciliation, they are in effect checking to see that the bank reconciliation was done. So it’s a control to check a control. That type of entity level control can also reduce the testing of other controls.

The third type of entity level control is the type that indicates the need to perform testing at the business process level and this is the most important type. For example, if you have a CFO who reviews the payroll register, then the auditor need not perform some detail testing maybe within payroll because the CFO review is adequate and the CFO is thorough and sensitive enough but if anything was wrong within the payroll cycle, it would be detected by the CFO. So said another way, the CFO control replaces other controls within the business process so you do not have to and saving time in the process.

Those are the type of so-called precise entity-level controls that we want to put in place because it can save a whole lot of time in testing.

### Precise Entity-Level Controls

- **Purpose** – to prevent or detect misstatements
- **Granular** – performed at Product line or location level
- **Consistent**
- **Specific assertion**
- Investigates amounts well-below materiality
- **Good comparison to actual results**

The chart above shows the requirements if you intend to use a precise entity-level control to replace business process controls at a small company.

First, the purpose of the control is to prevent or detect misstatements within a business process.

Second, the level at which the control has to be performed is granular enough to prevent or detect an error.

Third, the control must be performed consistently.

Fourth, the control has to satisfy a specific assertion.

Fifth, the control has to be sensitive enough, such that amounts well-below materiality are discovered and investigated.
Finally, the control provides a good comparison to actual results. An example of a precise entity-level control would be a comparison between actual results and either the prior year results or to a budget. The control would be performed on a periodic basis and the hard copy would be printed, with evidence of review and the investigation of items that are individually immaterial.

Preventing Management Override

- Maintain integrity and ethical values
- Increase oversight by the audit committee
  - Discuss/review significant estimates
  - Address override risk
- Whistleblower program
  - Receipt, treatment and retention of complaints
  - Required by SOX
- Monitor controls over certain journal entries
  - Restrict GL access
  - Dual authorizations
  - Review of entries made

Another problem that small companies face is management override. The following are four controls that can be put in place for prevention.

First, management must maintain integrity and ethical values at the company level.

Second, the audit committee should oversee the management, they should review significant estimates and they should address and monitor the risk that management is overriding controls.

Third, a whistle blower program can be put in place, so if management does intend to override controls someone would report that to the audit committee. This would be preventing management override—or at least detecting it once it has occurred. Whistle blower programs are, in fact, required by the Sarbanes-Oxley Act.

Fourth, top management who can override controls should not have the ability to make unilateral journal entries without approval. For example, journal entries could require dual authorization, which restricts general ledger access. Performing reviews of journal entries after the fact can detect management override as well.
Segregation of Duties

- **Ideal:** Separate authorization, recording, reconciling, custody of assets
- **Reality:** Small companies don’t have the personnel
  - Use external parties
  - Alternative controls
    - Review reports of detail transactions
    - Review selected transactions
    - Take periodic asset counts

Segregation of duties is also another issue within small companies; usually small companies do not have the personnel to be able to divide duties.

An alternative can be using external parties to perform some of the functions, like consultants.

Another solution can be putting specific alternative controls in place within the company. Examples of controls are having a review of detailed transactions and a review of selected transactions. Other controls include taking periodic asset counts such as fixed inventory accounts and asset accounts and then having a check done on reconciliations.

IT Controls

- **Less complex if:**
  - Manual controls over system outputs
  - Off-the-shelf software
  - Centralized processing, few interfaces
  - Simple spreadsheets
  - Outsourced

- **Risks:**
  - Bad data, bad processing
  - Unauthorized access
  - Unauthorized changes to data or programs
  - Updates not made
  - Manual intervention
  - Data loss (no backup)

In the information technology arena, smaller companies generally have less complex IT environments due to manual controls over system outputs, the use of off-the-shelf software, centralized processing with few interfaces, simple spreadsheets and outsourced IT functions.

Possible IT risks in a small company include: bad data accumulated or processed incorrectly, unauthorized users access the company’s information technology, unauthorized changes are made to programs or data, required updates are not performed and manual intervention occurs, or data is lost when
information technology is not properly backed-up.

To mitigate IT risks, small companies should have a limited number of resources supporting security over the company’s electronic data. Employees who are authorized to add or change permission levels within the IT systems should be limited. Those who are authorized to make changes to the software should be limited as well. Employees should monitor access to operating systems, data and software.

To prevent unauthorized access, the company should enforce password parameters so that passwords are required to be complex. User access should be changed only with written approval and terminated users should be promptly deleted from the system. Regular system backups should be performed.

### Accounting & Finance Competencies

#### Accounting & Finance Competencies

- Identify issues
  - New company activities
  - New accounting standards
- Proper GAAP
- Evaluate
  - Hiring criteria
  - Training
  - Performance reviews
- Just know their job and anticipate changes – not overall experts
- Consider using outside experts
  - Example: Review of tax accounting
  - Evaluate and monitor the expert

The PCAOB does not require that all employees in a small company be certified public accountants; however, the PCAOB does require small companies to have the capability to identify new accounting guidance and to be able to evaluate the impact of the new guidance on the company.

Employees should continually attend training to sustain and expand their accounting knowledge. Performance reviews should be performed on a periodic basis to evaluate the competencies of the employees and employees should know their job well and anticipate changes.

If a company does not have all of these competencies in-house, then management should consider hiring outside experts. For example, having an expert in tax accounting perform the tax provision may be preferable if the expertise does not exist in-house. However, when using an expert, SAS 73 requires that an evaluation of the expert be performed prior to the performance of their services and the expert should be monitored throughout the performance of their services.
SEC Interpretative Guidance

SEC Guidance for Small Companies

The new SEC guidelines mirror those from the PCAOB in requiring a top-down, risk-based approach.

SEC Interpretative Guidance

SEC Guidance Continued

The new SEC guidance focuses on starting with risks and then implementing controls to prevent those risks from becoming problems. Controls can either prevent or detect problems. Preventive controls keep risks from developing into problems, while detection controls find problems that have already occurred. As
long as the company 10-K or 10-Q has not been published in the interim, detection is an acceptable control under SOX.

With AS No. 5, the SEC also added an entirely new concept: consideration of the likelihood that a control will not operate properly. This means that the auditor must account for two kinds of risks: risks in the processes themselves, and risks that controls will fail.

On the one hand there is a risk inherent in processes, either because of the nature of the given process or because of any recent changes. For example, installing a new accounts payable system a month before the end of the year would create an inherent risk because the new system might still have some bugs to work out.

The second type of risk is the failure of a control. If, for example, the employee reconciling a bank account has no experience doing that job, the control may fail to catch mistakes.

The auditor must consider that some controls will not work, either because of human error, or because of new systems. This is a critical assessment for a risk-based approach.

While the SEC does not dictate a format for documenting controls it offers two recommendations. First, the auditor should not worry about documenting all controls, just the controls upon which the company relies, called "key controls." The controls that the company does not rely upon are called "non-key controls." Secondly, the audit documentation should identify the employee who performs each control. The guidance states that the SEC will accept the controls that a company puts into practice if they are documented following these two recommendations.

SEC Interpretative Guidance

SEC Interpretative Guidance
Testing Controls
- More evidence for high risk:
  - Bigger samples
  - More independent testers
  - More frequent testing
  - Keep evidence separately (binders)
- If less risk
  - Rely on monitoring: self-assessment
  - Knowledge & supervision by management (small companies only, need some evidence)
- Multiple Locations
  - High Risk – get more evidence
  - Low Risk – self-assessment, monitoring, central controls
  - Look at individual elements (accounts) by location
SEC Guidance: Testing Controls

Although the SEC will accept a company’s controls, the auditor must conduct more testing where risk is high. Where risk is low, the auditor can perform fewer tests or rely upon internal controls. In assessing a company with multiple locations, the auditor should gather more evidence from the high-risk locations than from the low-risk sites. Within each location, the auditor must assess risk at the process level.

In a practical example, if an auditor was measuring locations by revenue, and had a software development location in India, that site would have high engineering expenses but would have virtually no revenue if it sold nothing. As a result, it is important to look at the processes taking place at subsidiaries and remote locations, not just total revenue, total assets, or number of employees. The auditor must go beyond the locations to the processes themselves.

Should the auditor look at IT controls as well? Looking only at financial controls does leave the door open to someone hacking into the system and affecting the GL for example. What this means is that where IT controls could pose a risk to the financial side, the auditor must include them in the audit.

There are various frameworks for IT testing, but the most well known is CobiT, published by the IT Governance Institute. CobiT is like COSO in the sense that it describes an entire testing structure. A CIO following CobiT would have a strong IT organization. The IT Governance Institute wrote a number of good management practices into CobiT, but the SOX auditor need not follow all of them.

For instance, CobiT recommends evaluating all vendors. This is a good practice and makes sense to the degree that a vendor might potentially sell poor code or offer poor advice during a consultation, which could lead to financial problems for the company. However, auditors now generally recognize that implementing every CobiT management practice is unnecessary for SOX compliance. Despite being a great management practice, and a part of CobiT, a SOX auditor can omit vendor evaluation.

To summarize, there are some IT controls not directly linked to financial reporting controls that could lead to financial reporting risks. Chapter five covers these controls, but the reader should note that these definitely fall within the scope of Sarbanes-Oxley. Preventing hackers from exploiting IT controls is important because of potential consequences for financial reporting.

SEC Interpretative Guidance

- Indications of Material Weakness
  - Ineffective Control Environment
    - Sr. Management Fraud
    - SD unaddressed
    - Ineffective Audit Committee
  - Restatements due to correction
  - Auditor corrections
  - Ineffective regulatory compliance with material impact
- Give investors full assessment of impact of MW
SEC Guidance: Material Weaknesses

What is a material weakness? There are many hallmarks of a material weakness. One important indicator is an ineffective control environment. Three different issues can signal a material weakness within the control environment. The first is fraud by senior management. A compromised control environment, the CEO being indicted for instance, points to a material weakness.

Significant deficiencies that continue year after year without correction are a second indication of an ineffective control environment (The reader should remember that significant deficiencies are only reported to the board, not to shareholders). This situation is a material weakness because the continuation of the problem provides evidence that the management does not care enough to rectify the matter. If a significant deficiency exists, the company must address it; even if the significant deficiency is not cured, the company must make progress toward a solution.

A third instance of a material weakness within the control environment is an ineffective audit committee. An ineffective audit committee never meets or does not discuss required issues during meetings (there are lists of required issues).

In addition to an ineffective control environment, another important indicator of material weakness is restatement due to correction. Since the Act, roughly 36% of public companies have made restatements. Before the passage of the Act, only about 10% of companies made restatements in a given year; the change has been quite dramatic. The auditor already knows that the problem is material, because the company would not report it publicly if it were not material. This is prima facie evidence of ineffective controls, since proper controls would have caught such an error. As a result, this is a material weakness.

A restatement is always a material weakness. Many restatements arise out of carelessness or poorly trained employees, especially those restatements involving spreadsheet errors. These are simple mistakes, but they come to light with the restatement because no one scrutinized the process before. With Sarbanes-Oxley, auditors are investigating these processes and finding out about the little errors that add up. For instance, an incorrect depreciation taken for the last 10 years (even if it did not amount to much in any given year) can accumulate to a misstatement in net book value large enough that the company must report it to shareholders.

Two professors at the University of Hawaii, Raymond Panko and Richard Halverson, studied spreadsheet errors over a 20-year period and found that 86% of spreadsheets contain significant errors (Panko & Halverson, 1998, 2005). Panko and Halverson also found that most of the people who created the spreadsheets in the study thought that their own spreadsheets had no problems. This discrepancy means that while about 10% of the creators of spreadsheets think there might be a problem, 86% of the spreadsheets actually contain material errors (not just minor formatting mistakes).

Ineffective compliance with regulations is another marker of a material weakness. The three Ballentine circles on page 18 show that there can be an intersection between financial reporting and compliance with laws and regulations. The SEC now says that ineffective regulatory compliance could be a material weakness. (However, it is not clear that every instance of ineffective regulatory compliance is a material weakness. This raises a question: must the auditor examine compliance with every regulation governing the particular industry in which their client operates? Perhaps, especially in the case of banking where most if not all the regulations are financial regulations. On the other hand, it may not be necessary to investigate all the EPA regulations governing a waste disposal company. The reader can see that this is a tough question with no single correct answer. The rule that a regulatory compliance program must exist and the SOX team should ensure that the company has an effective program. However, the SOX team does not check for compliance with the requirements.

Finally, the SEC mandates informing investors of material weaknesses. This goes beyond simply stating that the audit found a material weakness; companies must also report to investors about the affected processes and offer a planned solution.
Chapter 2:
Project Scope, Schedule & Resources

Part 1: Documentation & Testing
Chapter 2 – Project Scope, Schedule & Resources

Documentation & Testing

Planning a New Project

One key to success for auditors new to SOX projects is seeking out the assistance of someone experienced in complying with the Act. Pooling existing knowledge through the creation of a roundtable of companies from the same industry that are willing to share their compliance strategies can offer valuable lessons. Finding companies that are not competitors is essential so that the information sharing process remains an open dialog. All of the roundtable participants can gain an understanding of some important questions, including: what to do, what kind of formats to use, who does the auditing work, what time frame is reasonable, and how deep should the review go? By answering these questions, the auditor can save a tremendous amount of effort in later stages of the project.

Having decided upon the scope, the next steps are documentation and testing. The auditor should begin documentation at the entity-level, and continue through business processes such as payroll, fixed assets, order entry, treasury, and closing the books. The auditor should also develop flowcharts and lists of risks and controls for each area mentioned.

One important term to keep in mind during the planning stage is “design deficiency.” A design deficiency is a risk that is found, even before testing starts, for which there are no controls. This means that the process was designed without the necessary controls to prevent all the existing risks. Design deficiencies must be fixed immediately because the auditor cannot test controls that have not been put in place.

A second type of deficiency, the operating deficiency, can show up during the testing phase. For example, the auditor finds a need for further controls if while examining bank accounts; he asks for reconciled accounts for the year only to find that beyond March, the accounts have not yet been reconciled. This indicates that the company filed a 10-Q without having reconciled the accounts for the given quarter. In short, an operating deficiency describes the situation in which a control fails during the testing phase.

What are the consequences of an operating deficiency? What happens when a test fails? In some cases, the employee performing the process must be retrained. In other instances, the process must be redesigned because the control does not in fact operate as it was written. The circular arrows in the diagram illustrate this continuous re-evaluation. Sometimes testing reveals the need for changes and new documentation, which in turn lead to re-testing.
Typically, during the first year a company complies with SOX, 30% of the tests fail. This increases the testing budget by about 30% as well, given the need for remediation and re-testing. However, by the second year, companies can often reduce the failure rate to 10%. The auditor must expect operating deficiencies occur quite often and account for them in the project plan.

Many times, companies will ask an auditor, “What is the best form of documentation?” Flowcharts are the best form of documentation. Narratives take a long time to prepare. In addition, producing a narrative that includes the necessary amount of detail will result in a long document. The auditor can describe the same procedures much more easily and quickly with a flowchart. Additionally, writing a narrative brings in the possibility of disagreement over language. Sometimes project team members disagree on narrative wording, and each wants to put his own editorial stamp on the document. Reconciling these differences adds time to the project without improving controls or testing.

One caveat to using flowcharts is that they must be prepared with attention to visual layout. Flowchart documentation prepared in a disorganized way or in a form that leaves out important elements can make even a well-done project unusable in the future. Chapter 3 covers flowchart preparation.
Chapter 2:
Project Scope, Schedule & Resources

Part 2: Project Guiding Principles
The chart above summarizes the important elements covered in this book. The first guiding principle is to limit the number of key controls. This does not mean that a company should remove controls. Rather it means that the SOX auditor should work with the controls necessary to achieve compliance. The reason for this is that every control needs retesting each year to ensure compliance with the Act. Fewer key controls mean less testing year after year. Techniques for maintaining an effective control structure with fewer controls will be covered later in the book.

The second guiding principle is to learn from others. Accelerated filers have experience with SOX, and learning from their knowledge is essential. Also, every industry has different processes and associated risks; the auditor can learn about starting a new SOX project by understanding how similar companies have complied. Thirdly, as mentioned earlier, the auditor should use expert knowledge, particularly during the planning phase. Experts can be most helpful by providing information on project organization, proper scope, and an appropriate timeline.

A third guiding principle is to leverage internal knowledge resources. Company employees know how processes work, and they know what controls ought to be in place. Who better understands the risks, and the controls designed to prevent those risks, than the process owners themselves? By interviewing these employees, the auditor can gain valuable information that would be difficult to come up with by analyzing the given process in isolation.

The fourth guiding principle is to design reusable project materials. Since SOX compliance is not a one-time experience, the auditor should design documentation and testing plans for re-use year after year. In addition, the auditor might need to implement the plan at several locations. If this is the case, any errors made at the first location will be replicated at each site. Thus, by designing an efficient, thorough procedure, the auditor can minimize the work necessary when he re-uses the plan in other locations and at other times.
Chapter 2:
Project Scope, Schedule & Resources

Part 3: Project Organization
Project Organization

The best way to get a project started correctly is to seek out an executive level sponsor such as the CFO. Having an executive sponsor will facilitate participation by middle management. Without the support of top management, lower-level employees are often less willing to help an auditor because they are already busy performing the required tasks of their job. However, if SOX compliance becomes a management initiative by virtue of having an executive sponsor, helping becomes part of the job for lower level employees. Similarly, the executive sponsor must support the project throughout its duration so that employees see compliance as a continuing priority.

After finding a sponsor, the next organizational element is the steering committee. While the steering committee does not carry out the project, it approves the budget and timeline. It makes decisions such as hiring external consultants versus using internal auditors. The steering committee members have enough authority within the company to allocate resources and to evaluate the progress of the project. The steering committee must also have the authority to approve changes to the budget. For example, at the project's inception, the auditor will present a top-down budget showing the amount of money and the areas in which it will be spent. Quite often, after the project has been started, the auditor must change the original budget as a bottom-up budget is developed with detailed lists of processes, controls, and tests. The steering committee must be able to review the project and either approve the budget changes or work with the project team on modifying the plan to fit the existing budget. For this reason, the steering committee and project manager should meet at least once a month.

The next organizational aspect is the project team itself. A project manager, with the responsibility of presenting the project status to the steering committee, heads the team.
Chapter 2 – Project Scope, Schedule & Resources

The project work takes place at the base of the organizational structure. The base includes the process owners and the documenters and testers. The documenters and testers interview process owners to find out how each process operates, document these steps, and then test them. Moreover, those working on the compliance project, whether internal auditors or external consultants should have familiarity with business processes and with preparing work papers.

External auditors are the final group that plays a part in project organization. The external auditors must be involved at every step of the project because they must approve decisions made at every level, from the executive sponsor down to the documenters and testers. For example, if the external auditors can approve a definition of materiality at the start of the project, they will not come back, well into the project, requiring that new processes be added to the scope of the project. This is important for fixing the scope of the project. Changing the scope midway through a project because the auditors did not accept the standard of materiality could require tremendous effort to update the documentation and testing procedures.

It is a good practice to meet with the external auditors every two weeks, or at least once a month, to keep them apprised of the details of the project. This allows the project team and the external auditors to coordinate their activities.

Oversight

<table>
<thead>
<tr>
<th>Oversight</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review Committee</td>
</tr>
<tr>
<td>- Evaluate gaps and decide remediation required</td>
</tr>
<tr>
<td>- Skills required- knowledge of GAAP, COSO, PCAOB standards; public company SEC reporting experience</td>
</tr>
<tr>
<td>Steering Committee (some members may overlap the Review Committee)</td>
</tr>
<tr>
<td>- Approve the scope, schedule, and resources of the project</td>
</tr>
<tr>
<td>- Monitor the project’s progress as reported by the project manager</td>
</tr>
</tbody>
</table>

Skills required – financial executive-level decision-making, leadership, influence and communication skills

Project Oversight

The review committee is the group that evaluates the significance of deficiencies found during the project. Review committee members may be part of the steering committee but should have extensive knowledge of GAAP. When composing a review committee, the auditor should start with the people who review the company's financial statements.

Beyond the number of deficiencies, the review committee will also want to know how many of these problems the project team or process owners can fix by the end of the year. Further, the review committee will need to know how many of the deficiencies will create serious difficulties for the company. The review committee would consider any material weaknesses or significant deficiencies to be serious problems.
Chapter 2: Project Scope, Schedule & Resources

Part 4: Project Team Staff
Documenters & Testers

The documenters and testers are the people who will evaluate the company’s risks and controls. They will perform the necessary sampling procedures and prepare the work papers and flowcharts documenting the project. Documenters and testers must have great communication skills along with solid knowledge of business practices because the project will require them to interact with employees at all levels of the organization, from executives to the receiving department. Documenters and testers should also have auditing experience.

Documenters & Testers

- Interview process owners
- Prepare flowcharts
- Propose financial risks
- Evaluate and document controls
- Develop conclusions as to the design of controls
- Select samples and perform testing
- Recommend operational process improvements

Skills required – Understanding of business process relevant to the
The project manager must be able to build a team and keep that team motivated for the duration of the audit. He must also be able to manage the budget and keep the team working within that budget. The project manager needs excellent communication skills to present status reports to company management. He may review work done by team members as well. Ideally, on a large-scale project, another team member would conduct such reviews, but on smaller projects, this duty might fall to the project manager. He also plays a central role in publicizing the project and supporting it across the company. For instance, some groups within the organization will want to learn what to expect during the documentation phase, as they are unfamiliar with SOX; the project manager should be able to explain the procedures to help build support for the project.

Additionally, the project manager is responsible for designing the format of the work papers and flowcharts that will document the project. He must train the team and manage team members on a daily basis. Moreover, he is the liaison with the steering committee, the one who will make suggestions concerning project scope. Finally, the project manager approves testing procedures and reports deficiencies to the steering and review committees.

The project manager’s role includes an extensive range of duties, which requires excellent interpersonal skills, the ability to conduct training, and the ability to make dynamic and concise presentations. Moreover, he must have sound accounting knowledge as well. In short, the project manager’s responsibility covers many of the judgments that will lead to the success or failure of the project.
On a project of any size, a librarian can save money. The librarian keeps track of all the details of the project. In a large project with hundreds of controls, monitoring how much of the budget has been spent, which controls have been tested and which have not, or which tests have passed and which have failed, make having a librarian essential. The librarian also keeps track of the documentation and other work papers that the project team produces.
Chapter 2: Project Scope, Schedule & Resources

Part 5: Materiality
Materiality: Common Quantitative Factors

<table>
<thead>
<tr>
<th>Materiality: Common Quantitative Factors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revenues</td>
</tr>
<tr>
<td>Net income</td>
</tr>
<tr>
<td>Current assets</td>
</tr>
<tr>
<td>Equity</td>
</tr>
</tbody>
</table>

- Method depends upon the users of the financial statements
- A public company would typically use net income as the critical factor.
- Adjust for one-time items and tax effect

Determining Materiality

There are several techniques for determining materiality, and choosing the appropriate one depends upon the type of company involved. For instance, a company that is losing money but has extensive assets might determine materiality in relation to equity. A fast growing high-tech company might use revenue or a percentage of net income to determine materiality.

The auditor must consider other factors in determining materiality as well. For example, if a company has decided to use net income to determine materiality, it must not simply take the net income figure at face value. If the company in question had a net income of $65 million, the auditor should realize that this is an after-tax figure. As a result, the company should not use $65 million, but should add back the 35% statutory tax rate to that amount before using it to calculate materiality.

Having calculated the company’s income before taxes, determining materiality next requires the auditor to examine the financial statements for any one-time expenses in the base year that might have lowered income. For example, if the company had made an adjustment under FASB Statement 123(R), the auditor might want to add that expense back into the income calculation if the company does not expect similar expenses on a regular basis. If the auditor does not add such one-time expenses back into income, he will end up calculating an artificially low threshold for materiality.

Lastly, if a company makes a budget plan for the next year, the auditor can use that to calculate net income. These examples show that the auditor must make several different judgments about the company and its financial status to determine materiality.

Finally, as mentioned in chapter 1, the auditor should determine a judgment materiality, not a definitive standard. Judgment materiality means that the auditor must analyze the circumstances surrounding any eventual weaknesses as well. If for example the judgment materiality is $5 million, then any process relating to financial reporting that has at least that much money flowing through it will be within the scope of the project. The process of setting the scope is still subject to management judgments; company managers may wish to include processes or locations where less than $5 million are involved.
Chapter 2: Project Scope, Schedule & Resources

Part 6: Documentation and Testing – Processes vs. Risks
Chapter 2 – Project Scope, Schedule & Resources

Documentation and Testing Details

Identifying Areas for Documentation

After determining a judgment materiality, the auditor can begin documentation. The diagram above brings back the pyramid shown earlier in this chapter to remind the reader of the hierarchy generally used in SOX projects. The key aspect of this pyramid is that each step builds upon the foundation laid by the previous one.

Within the documentation and testing portion of the project (highlighted in blue in the illustration), the reader should note a one-to-many relationship. First, the auditor must identify all of the locations, including parents and subsidiaries. The processes to be documented take place within each location. There are risks, as well as controls designed to prevent those risks from occurring, within each process. Finally, the auditor must test each key control to ensure that it functions as designed.

A brief look at the expenditure cycle can give the reader a clearer understanding of processes. The expenditure cycle requires setting up vendors, issuing requisitions, making out purchase orders, receiving the goods ordered, matching for payment, and reconciling the accounts at the end of the month. Each of those parts of the expenditure cycle is a process. The reader should note that certain companies use the term “process” to refer to what this book calls a cycle. These companies refer to the processes within a cycle as “sub-processes.” These terms are equivalent to the cycles and processes discussed in this book.

In the expenditures example above, each process within the cycle can have one or more risks associated with it. For instance, in relation to the purchase order process, blank forms could be stolen, signatures could be forged, or purchase orders could be copied in order to divert a second payment check. The auditor must consider all possible risks within a given process (a logical method for determining risks will be discussed later). Then the auditor must identify at least one control for each risk. Sometimes one control can be used to prevent multiple risks; the holy grail of SOX risk assessment is finding controls that cover multiple risks.
Processes vs. Risks

The diagram above represents the same information contained in the pyramid on page 53 in a slightly different format. It is presented in two forms because understanding the terms involved in documentation is critical to the entire SOX project.

The chart above depicts a parent company located in the United States with subsidiaries spread around the world. Each location keeps its own general ledger (GL). Each GL contains hundreds of accounts. The row highlighted in blue shows the expenditure cycle discussed on the previous pages, including preparation of requisitions, receipt of goods, receipt of invoices from the vendor, matching invoices to requisitions, and payment. The chart shows each process connected to the next because every accountant may have his own understanding of the cycle, and thus delimits the various processes within it differently from his peers. As a result, documentation must be explicit so that by seeing the cycle on paper, one can clearly understand the boundaries of each process. Clear delineation of processes helps the project team avoid reviewing elements of one process twice or skipping others entirely.
Chapter 2 – Project Scope, Schedule & Resources

The gray highlight around the first two processes represents the idea that multiple processes can be documented with one flowchart. Where possible, the auditor should document more than one process on one flowchart to reduce the number of files within the SOX project. A smaller number of files makes organization much easier.

The small green boxes underneath the processes represent employees carrying out activities within each process. In general, employees tend to think little about the process, focusing solely upon their piece of the puzzle. Some employees will perform activities that create transactions appearing on the financial statements. For example, when an employee pays a bill, he will debit accounts payable and credit cash. This appears in the financial statements while many other transactions, such as issuing purchase orders, do not.

There are no transactions listed in the first process that show up in the financial statements. This will often be the case, and while sometimes these processes can be taken out of the scope of the project, often they must be included. Even if it contains no transactions appearing in the financial statements, the auditor must include a process in the project if the company relies upon controls within it.

For instance, in the case above, if the employee receiving goods relies upon having a valid purchase order, which in turn relies upon a requisition signed by the manager, then the PO process must be included in the scope of the project. Transactions later in the cycle rely upon controls on previous transactions and previous processes. On the other hand, if the company operated on a non-PO basis, which is to say that the signed invoice is taken as an implicit authorization to purchase the given goods, the auditor could omit the first two processes from the scope of the project.

The auditor should look at the transaction level to identify potential risks. To revisit an earlier example, the PO process might contain the risk of someone stealing a blank purchase order form and forging a signature to order goods or services without authorization. Keeping the PO forms in a locked cabinet is a potential control for this risk. This is an example of a manual control, one that does not involve an IT system.

If an employee in receiving could claim a whole shipment was received when in reality only half of it arrived, but there is no control to prevent this from happening, the auditor has found a design deficiency.

Perhaps someone in Accounts Payable can forge an invoice that looks valid and enter it into the A/P system. This risk might have an IT control; the company may program the computer system to accept only invoices that match valid purchase orders. IT controls are also known as automated controls. Controls that combine manual and automated aspects, such as having an employee review reports generated by the IT system, are called hybrid controls.
Chapter 2: Project Scope, Schedule & Resources

Part 7: Hierarchy
Hierarchy of Sarbanes-Oxley Project Elements

The diagram above represents the hierarchy of elements essential to a successful SOX project. These same ideas are depicted in the diagram on the previous pages. The center of this diagram also includes a box labeled “objectives.” The auditor can only understand how to evaluate the transactions, the risks involved, and the controls implemented to prevent those risks if he knows the objectives of the given process.

For example, if a company gives the auditor its financial statements along with the assertion that the statements are correct, the auditor has only perhaps a vague idea of what correct means. Does this mean that they comply with GAAP? Even if this is what the company means by “correct,” such an assertion relies upon many implicit assumptions. It assumes that all of the appropriate expenses have been entered correctly; it assumes that the company actually owns all of the assets listed; and it assumes that all estimates have been made properly and with good judgment. This assertion therefore relies upon assumptions about a range of processes. The auditor must consider the objectives of each of these processes in order to evaluate the “correctness” of the financial statements.

At the process level, one potential objective in the vendor setup process is ensuring that none of the listed vendors are fictitious. In other words, the objective is a positive restatement of a risk. Understanding the concept of an objective is important because some companies choose to work toward objectives rather than to think about preventing risks. These same companies may also emphasize controls. If that is the case, the company is implementing controls to prevent the risks from becoming problems without explicitly
labeling the risks. Other companies emphasize risks and using controls to prevent those risks. These companies often do not discuss the objectives of the controls they have implemented.

A better practice is to consider the objectives of a given process, assess the risks that could keep the company from achieving those objectives, and then identify specific controls to prevent those risks.
Planning a SOX project raises many questions. For instance, companies often ask how much the project will cost. The sample spreadsheet shown above represents a SOX project for a very small company with only one location. The reader might find it surprising that, even on a small project, the total cost can amount to over $500,000.

The spreadsheet lists six cycles at the sample location; for instance: expenditures, payroll, financial reporting, fixed assets, order entry or revenue, and treasury. Within each cycle, there are 10 processes; this represents an average number of processes that the auditor could expect to find in a given cycle. However, the number of processes could easily be higher in cycles such as revenue, or lower in cycles such as fixed assets.

There are three objectives within each process, and each of these objectives contains two risks. To simplify a bit, this means that there are six risks per process (multiply the number of objectives by the number of risks per objective). Thus, the auditor must document 360 risks in the project.

If, for the sake of the sample, each risk had one unique control (this assumes that no controls prevent more than one risk), the auditor must test 360 controls.

---

**Minimum Project Size**

Planning a SOX project raises many questions. For instance, companies often ask how much the project will cost. The sample spreadsheet shown above represents a SOX project for a very small company with only one location. The reader might find it surprising that, even on a small project, the total cost can amount to over $500,000.

The spreadsheet lists six cycles at the sample location; for instance: expenditures, payroll, financial reporting, fixed assets, order entry or revenue, and treasury. Within each cycle, there are 10 processes; this represents an average number of processes that the auditor could expect to find in a given cycle. However, the number of processes could easily be higher in cycles such as revenue, or lower in cycles such as fixed assets.

There are three objectives within each process, and each of these objectives contains two risks. To simplify a bit, this means that there are six risks per process (multiply the number of objectives by the number of risks per objective). Thus, the auditor must document 360 risks in the project.

If, for the sake of the sample, each risk had one unique control (this assumes that no controls prevent more than one risk), the auditor must test 360 controls.
To summarize, after the planning stage, the project consists of two phases: documentation and testing. The biggest cost in the documentation phase is the number of processes that must be documented. The project team must assess how many flowcharts, and how many risk and control matrices, they must produce. Then the team must calculate the time they will need for these documentation tasks.

The spreadsheet lists 8 hours for documenting each process. That is a good goal to aim for, but within that timeframe, the team must identify all of the risks and controls in the process, develop a flowchart, interview the employees, draw the flowchart using Visio™, describe all of the risks and controls, and check the results by reviewing them with the process owners.

If the project team can document each of the 60 processes in 8 hours, they can complete the documentation phase in 480 hours. Because documentation requires the ability to run meetings, conduct interviews, and understand internal controls, management-level team members are needed. The spreadsheet here lists an hourly rate of $115, which might even be low for someone with the necessary qualifications. As a result, the cost of documenting all processes is $55,000.

At nearly $1000 per process, the documentation budget emphasizes the importance of limiting the scope of a project. Testing adds even more to the total project cost.

The figure of 7.4 hours per test (shown on the spreadsheet) is another average, calculated across the range of Cost Advisers, Inc. clients. The reader may ask if this number decreases on a project where many of the controls are IT controls, which can take as little as one hour to test. Statistically speaking, the average would change little, because some manual controls will take much longer than 7.4 hours to test.

If the project team has written a detailed, effective testing plan explaining the exact procedures testers should follow, including the details for which they should be looking, the high level personnel required for documentation are not necessary. For this reason, the billing rate for testing is only listed at $70 per hour. Testing controls then adds another $186,000 to the budget.

The reader should note that this does not include testing IT general controls (ITGC). The 300 hours added for IT testing is a conservative estimate, and teams new to SOX will likely spend more time on this part of the project. Even with this conservative estimate, ITGC testing adds another $34,500.

The next project element is the examination of the segregation of duties. This means verifying that those employees conducting transactions do not also implement controls. Segregation of duties analysis requires collecting data from the IT systems and developing conflict tables (these will be discussed later in the book). This step will add another 200 hours ($23,000) to the budget.

As mentioned above, a librarian plays a vital role in keeping track of the various elements of the project. On a six-month project, the librarian adds $25,000 to the budget.

Finally, given the wide range of expertise that the project manager must have, $150 per hour is a reasonable rate for the team leader. This adds yet another $208,980 to the budget.

Given the conservative estimates and small size of the project portrayed here, the reader can get a sense of how expensive SOX compliance can be. As a result, the auditor must limit the scope of a project at the planning stage.

Reducing the number of processes in the audit is one way the project team can limit the scope of the project. Eliminating just 10% of the processes in the examples shown reduces the cost of the project by $50,000. The impact comes not just in terms of the number of processes that the team must document and test, but also in terms of the number of hours for which the team must bill, including the librarian and project manager.

Another way to cut costs is to use internal resources to do testing where possible. For example the accounts receivable manager could test accounts payable and the accounts payable manager could test accounts receivable. Also, if the company has subsidiaries, the controllers could be rotated between the subsidiaries to do testing.

A third method of limiting project expense is a risk-based approach. While the team might spend 7.4 hours testing the high-risk controls, they might spend less time on the controls implemented to cover smaller risks.
These techniques can help companies reduce the cost of SOX compliance. The high cost is one of the reasons that small companies complained so much about the Act early on. The reader should note that the external auditor is not listed on the spreadsheet example, and would add another large sum to the budget.
Identifying the Process Population

The diagram above shows one way for project teams to decide on the processes to include within the scope of the project. A more technical method will be discussed later, but the project team can make an informal decision by looking at a list of processes from a similar company, and using those processes that apply to the case at hand (for a sample list of processes, see Appendix A). The auditor can map the processes against company financial statements to ensure that he has included all of the necessary processes. Also, the auditor can review the list of processes with company representatives. These verification measures help the auditor ensure that the scope of the project covers all of the appropriate processes.

One issue to keep in mind is that having two locations does not mean double the number of processes. If for instance, one company buys out another company, but each produces different products, it might be necessary for the company to keep the locations separate. However, the company will centralize corporate level processes like issuing the 10-K or treasury. As a rough guide, the auditor could expect to have about 50-120 processes within the scope of the project.
Chapter 2: Project Scope, Schedule & Resources

Part 9: Account Risk and Assertions
Account Risk & Assertions

Risk Assessment Matrix 1. Risk Identification and Analysis by Account and Disclosure

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>BALANCE SHEET</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Assets</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cash &amp; Cash Equivalents</td>
<td>6%</td>
<td>M</td>
<td>H</td>
<td>M</td>
<td>H</td>
<td>M</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Accounts Receivable</td>
<td>50%</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>L</td>
<td>H</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Prepaid Expenses</td>
<td>4%</td>
<td>L</td>
<td>M</td>
<td>L</td>
<td>L</td>
<td>L</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Inventory</td>
<td>35%</td>
<td>H</td>
<td>M</td>
<td>M</td>
<td>L</td>
<td>M</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Property &amp; Equipment</td>
<td>13%</td>
<td>H</td>
<td>L</td>
<td>L</td>
<td>L</td>
<td>L</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Intangible Assets</td>
<td>10%</td>
<td>H</td>
<td>M</td>
<td>M</td>
<td>M</td>
<td>M</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Total Assets</td>
<td>100%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Liabilities</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Accounts Payable</td>
<td>59%</td>
<td>H</td>
<td>M</td>
<td>L</td>
<td>M</td>
<td>M</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Accrued Expenses</td>
<td>13%</td>
<td>H</td>
<td>M</td>
<td>M</td>
<td>H</td>
<td>H</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

Source: COSO Internal Control over Financial Reporting – Guidance for Smaller Public Companies
Volume III = Example of Pre-filled forms
Volume IV = Blank Forms

Significant Accounts

The method described above is probably the most straightforward way to identify processes, but the PCAOB and SEC refer to another technique. They use the term Significant Accounts. The Significant Accounts method requires identifying the accounts to which processes contribute.

The concept used in this method is mapping the processes to the accounts that they affect. Mapping simply means identifying the accounts that are affected by each process. The auditor does this by listing all of the accounts in a single spreadsheet column and all of the processes in a row across the top of the spreadsheet. Then the auditor can check off the processes that are involved in each account. If, after completing the mapping procedure, the auditor finds accounts that have no processes mapped to them, he knows that more processes must be added to the list. The mapping procedure is a systematic means of checking to see that all of the necessary processes have been included in the project.

Mapping is also important because it allows the auditor to identify the accounts affecting a particular process. This can help the auditor to gain a sense of the dollar amount of materiality that is relevant to a given process. By examining the amounts in the accounts affected by a process, the auditor can begin to understand the importance of that process in relation to the project as a whole.
The third reason for using the mapping technique is more complex. An earlier example in this chapter discussed the assumptions underlying “correct” financial statements. That is to say, the auditor can examine some concrete elements to verify the financial statements. The chart above (which comes from the COSO Small Business Guidance, mentioned in chapter 1) lists these elements in the columns at the right of the table (in abbreviated form): existence (E), completeness (C), valuation and allocation (V/A), rights and obligations (R&O), presentation and disclosure (P&D). The auditor can use these five criteria to determine whether a financial statement is correct. The principle behind these assertions is that the auditor will go through the financial statements account by account to note which assertions are relevant in each instance.

In the first row, the reader will see the account Cash & Cash Equivalents. Existence is relevant. Completeness is also relevant and the auditor must ensure that all cash accounts figure in the number presented in the financial statements. Valuation is not relevant to cash as it involves estimates and judgment. To assess the Rights and Obligations assertion, the auditor must ask, “Does the company actually own the cash in its accounts?” Hopefully this is not a problem, but it is clearly relevant. Presentation and Disclosure assertions are also relevant; the auditor must ask if credit balances or cash accounts have been reclassified as liabilities on the balance sheet.

Of the five standard assertions, four are applicable to this case. Those who work with SOX call these four assertions “relevant assertions.” This term is straightforward; these assertions are relevant to the account under scrutiny. Until COSO published these assertions in its Small Business Guidance, the auditor had to come up with the relevant assertions on his own. Now however, the auditor can look to this guide and use COSO’s determination of the relevant assertions based upon report groupings.

Determining relevant assertions is important, because if the auditor can map assertions not only to accounts, but also to processes, he will have a much easier task identifying objectives and conceptualizing the risks involved. Applying the relevant assertion of Completeness to the Cash account, all of the cash balances within the company must be listed in the Cash and Cash Equivalents account. In a sense then, the objective is the relevant assertion written out as a sentence. While the assertion is one word, the objective puts that attribute into a sentence to state it more clearly in terms of a specific process. For example, “The objective is for all company cash accounts to be included in the cash balance.”

Because the risk is the opposite of the objective, the risk is that not all of the cash accounts are included in the presentation of Cash and Cash Equivalents. By identifying all the assertions by account and all the accounts by process, the auditor can be certain of uncovering all of the risks involved. The COSO Small Business Guidance is a valuable tool that can save the auditor a great deal of time in identifying relevant assertions.
SAS 106 expanded the five assertions used in the COSO model. SAS 106 expands the number of assertions and classifies them into three categories: Transactions and Events, Account Balances and Presentation and Disclosure. The table below outlines the assertion and impact on the financial statements. Using the assertions outlined in SAS106 may add efficiencies to the SOX project as the company’s external auditor will likely use the new guidance in the audit of the financial statements.

**Transactions & Events**

<table>
<thead>
<tr>
<th>Assertion</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Completeness</td>
<td>All transactions and events that should have been recorded have been recorded.</td>
</tr>
<tr>
<td>Cutoff (Proper Period)</td>
<td>Transactions and events have been recorded in the correct (proper) accounting period.</td>
</tr>
<tr>
<td>Accuracy</td>
<td>Amounts and other data relating to recorded transactions and events have been recorded appropriately.</td>
</tr>
<tr>
<td>Classification</td>
<td>Transactions and events have been recorded in the proper accounts.</td>
</tr>
<tr>
<td>Occurrence / Authorization</td>
<td>Transactions and events that have been recorded have occurred and pertain to the entity. Transactions and events have been authorized in accordance with management's intentions.</td>
</tr>
</tbody>
</table>

**Account Balances**

<table>
<thead>
<tr>
<th>Assertion</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Completeness</td>
<td>All assets, liabilities, and equity interests that should have been recorded have been recorded.</td>
</tr>
<tr>
<td>Valuation &amp; Allocation</td>
<td>Assets, liabilities, and equity interests are included in the financial statements at appropriate amounts, and any resulting valuation or allocation adjustments are properly recorded.</td>
</tr>
<tr>
<td>Rights &amp; Obligations</td>
<td>The entity holds or controls the rights to assets, and liabilities are the obligations of the entity.</td>
</tr>
<tr>
<td>Existence</td>
<td>Assets, liabilities, and equity interests exist.</td>
</tr>
</tbody>
</table>

**Presentation & Disclosure**

<table>
<thead>
<tr>
<th>Assertion</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Completeness</td>
<td>All disclosures that should have been included in the financial statements have been included.</td>
</tr>
<tr>
<td>Understandability &amp; Classification</td>
<td>Financial information is appropriately presented and described and disclosures are clearly expressed.</td>
</tr>
<tr>
<td>Rights and Obligations, and Valuation and Accuracy</td>
<td>Disclosed events and transactions have occurred and pertain to the entity. Financial and other information are disclosed fairly and at appropriate amounts.</td>
</tr>
</tbody>
</table>

Safeguarding of Assets: when not applicable to a specific transaction, add as an applicable assertion. For example, maintaining check stock in a secure location is a safeguarding control but not applicable to a specific transaction.
Chapter 2:
Project Scope, Schedule & Resources

Part 10: Process to GL Map
Process to GL map

**Risk Assessment Matrix 2. Risk Analysis Mapping Accounts to Business Processes**

<table>
<thead>
<tr>
<th>Financial Statement Account</th>
<th>Cash &amp; Cash Equivalents</th>
<th>Accounts Payable</th>
<th>Retained Earnings</th>
<th>Product Sales</th>
<th>Compensation and Related Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Business Process</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GL Closings &amp; Reporting</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>General Ledger Maintenance</td>
<td>H</td>
<td>M</td>
<td>M</td>
<td>H</td>
<td>M</td>
</tr>
<tr>
<td>Non-Recurring Transactions</td>
<td>H</td>
<td>M</td>
<td>M</td>
<td>H</td>
<td>M</td>
</tr>
<tr>
<td>Period Close</td>
<td>H</td>
<td>M</td>
<td>M</td>
<td>H</td>
<td>M</td>
</tr>
<tr>
<td>Foreign Currency Translation</td>
<td>H</td>
<td>M</td>
<td>M</td>
<td>H</td>
<td>M</td>
</tr>
<tr>
<td>Consolidations</td>
<td>H</td>
<td>M</td>
<td>M</td>
<td>H</td>
<td>M</td>
</tr>
<tr>
<td>Financial Statement Preparation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Accounts, Management Estimates, and Reserves</td>
<td>H</td>
<td>M</td>
<td>M</td>
<td>H</td>
<td>M</td>
</tr>
<tr>
<td>Goodwill and Other Intangibles</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC Filings and Other Regulatory Disclosures</td>
<td>H</td>
<td>M</td>
<td>M</td>
<td>H</td>
<td>M</td>
</tr>
<tr>
<td><strong>Treasury</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cash Management</td>
<td>H</td>
<td>M</td>
<td>H</td>
<td>H</td>
<td>M</td>
</tr>
<tr>
<td>Investment Securities</td>
<td>H</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Revenue &amp; Receivables</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Order Processing</td>
<td>H</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shipment</td>
<td>H</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cash Receipts</td>
<td>H</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Invoicing</td>
<td>H</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Credit Notes and Adjustments</td>
<td>H</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Purchasing &amp; Payable</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Purchasing to Payables</td>
<td>H</td>
<td></td>
<td></td>
<td>M</td>
<td>H</td>
</tr>
<tr>
<td>A/P and Cash Disbursements</td>
<td>H</td>
<td></td>
<td></td>
<td>M</td>
<td>M</td>
</tr>
</tbody>
</table>

Source: COSO Internal Control over Financial Reporting – Guidance for Smaller Public Companies
Volume III = Example of Pre-filled forms
Volume IV = Blank Forms

**Mapping Processes to Financial Statement Groupings**

The diagram discussed on the previous pages mapped assertions to accounts; the chart above maps processes to financial statement groupings. This chart also shows an example of a cycle labeled as a process and a process labeled as a sub-process, but the principle remains intact. In the first column, the reader will see the cycles; the second column lists the processes within those cycles; and the row at the top of the chart lists financial statement accounts.

Note: The chart on page 65 showed a check mark in the appropriate column to map an assertion to an account. The chart on this page uses H and M instead. These stand for High risk and Medium risk (Low risk is not shown on this chart). Determining the level of risk will be covered later in this book, but for now what is important is linking a particular process to a given account (marked either by an “H” or an “M” on the chart).
Mapping Assertions to Processes

The diagram above shows the link between the two previous charts. The first chart (on page 65) mapped assertions to accounts. The second chart (on page 69) mapped processes to financial statement accounts. Now, having connected both processes and assertions to financial statement accounts, the auditor can associate assertions with processes. Knowing which assertions are relevant to each process allows the auditor to define objectives for each process since the assertions are one-word identifiers of objectives. The auditor can then turn these objectives into risks by asking the question, “What could go wrong on the way to achieving the given objective?” This method gives the auditor a systematic means for identifying all of the risks that he must document.

To summarize, the first step is to map GL accounts to processes. Secondly, the auditor can use the COSO Small Business Guidance to identify the relevant assertions for each account. Then he can associate relevant assertions to each process. Finally, by turning the assertions into objectives and the objectives into risks, the auditor can be certain of creating a rigorous documentation plan.

Now that the reader knows the procedure, it is not usually necessary to go through all of these steps. Because SOX has been around for a few years now, much of this work has already been done. By finding others in one’s network who have completed compliance projects or by talking with consultants, the savvy auditor can avoid starting from scratch by sharing what others in the industry have done. Unless the processes are industry specific, chances are good that someone out there has already compiled the pertinent information. However, by understanding this technique the auditor can properly assess the risks in all industry-specific processes involved in a given project.
Chapter 2: Project Scope, Schedule & Resources

Part 11: Project Timeline
Building a Project Timeline

The diagram above represents a timeline from an actual SOX project. The auditor must present a document like this to the company's steering and audit committees. This particular timeline is for a company operating on a calendar year. The auditor has coded the tasks on the timeline according to the hierarchy shown in the pyramid at the bottom left. The project team plans the project early in the year. By the end of the second quarter, the project team should be done planning and determining the scope and should start the documentation phase. The team should complete documentation by the end of the third quarter at the latest so that they can begin testing.

The reason that the chart shows some testing during the third quarter is to uncover any problems well before the end of the year. The project team will find testing exceptions and design deficiencies that they need to correct. SOX gives some latitude to companies trying to comply for the first time. If the company can fix a material weakness by the end of the first year, it is not required to include that MW in the annual report. Beyond the first year, however, any material weakness must be disclosed even if the company fixes them before the end of the year. It is for this reason that the timeline shows an early completion date for the project.

One important aspect of SOX that the timeline does not represent is “roll-forward testing.” Roll-forward testing means that most of the testing should be completed near the end of the year (ideally during the third quarter) because the CEO and CFO must sign the assertion statement at the end of the year. If testing is done too early in the year, the company runs the risk of making changes that could affect the controls that have already been verified. In other words, if a company implemented a new accounting system during the third quarter after testing in the second quarter, the executives would be signing an assertion statement based upon the old system that would not reflect the changes made. In short, if testing is done too early, there is no guarantee that the processes would still be operating the end of the year.
Companies can do some early testing for section 302 of the Act, the quarterly assessment. Companies often identify high-risk processes and test them nearly every quarter. They usually do very little testing during the first quarter, but will conduct some tests during the second and fourth quarters, saving the bulk of the testing for the third quarter.

Often external auditing firms will require that the project team withhold a sample from the third quarter testing to be verified during the fourth quarter. The danger with this method is that the third quarter testing may pass, but the sample reserved for the fourth quarter might contain problems. In that situation, the company might not have the necessary time to fix the problem and would have to report a material weakness to shareholders.

The reader should also note that the color-coding representing the external auditing phase on the diagram starts out light and gets darker toward the end of the year. This represents external auditor involvement throughout the project. As mentioned earlier, the project manager should try to keep the external auditors involved throughout the project because if external auditors suggest scope changes toward the end of the year, the project team will have great difficulty adjusting. The project manager should explain the scope, documentation, testing time frame, and findings (including deficiencies that are not significant deficiencies or material weaknesses) to the external auditors along the way. This will help avoid any surprises that could compromise the project late in the year.
Chapter 3:
Section 1 Analysis of Risks and Controls

Part 1: Wedding Cake-Entity Level Controls
The ‘Wedding Cake’

The “wedding cake” diagram shown above represents a different visualization of the information in the COSO Cube. The bottom layer of the cake shows company-level controls, also called entity-level controls and “tone at the top.” In chapter one, this was the bottom layer of the COSO Cube (called Control Environment). The next layer of the cake is IT infrastructure, which includes the network used, data center servers, operating systems, intrusion detection, and backup; in short, all of the concerns of the IT department. The layer above IT infrastructure is IT applications; these are the software packages that the company uses, such as the GL, A/P and payroll modules.

The reason for the distinction between IT infrastructure and IT applications is that business processes, the top layer of the cake, rely heavily upon IT applications. For example, a company relies upon many different reports. Completing a reserve for bad debts requires producing an aging report out of the order processing system in the accounts receivable module. Because of the close relationship between business processes and IT applications, the auditor must consider these two layers in tandem during the documentation procedures.

On the other hand, the auditor should consider IT infrastructure separately from business processes during documentation. The sample budget developed in Chapter 2 included a separate line for IT testing. Testing the IT infrastructure is a separate block of work, and thus is distinct from IT applications in the diagram above.

Why represent the project structure as a wedding cake with layers stacked on top of each other? Theoretically, and in most practical cases, a problem with the IT infrastructure means that the company can neither rely upon its IT applications nor trust its business processes (which are affected by IT applications). Each layer depends upon the foundation beneath it. If it is possible for a hacker to get into the company database and change A/R records, then any aging report generated will be incorrect. Employees relying upon this report to write a bad debt reserve entry will be basing their work upon flawed information. As a result, any problems with IT infrastructure must be evaluated in terms of their influence on IT applications.
and business processes. However, the auditor will document IT applications and business processes together, but he will document IT infrastructure and entity-level controls as separate pieces of the project.

Examples of Entity-Level Controls

<table>
<thead>
<tr>
<th>Entity-Level Controls</th>
<th>HR Policies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrity &amp; ethics</td>
<td>Hiring Guidelines &amp; Procedures</td>
</tr>
<tr>
<td></td>
<td>New Employee Orientation</td>
</tr>
<tr>
<td></td>
<td>Background Checks</td>
</tr>
<tr>
<td>Board of Directors</td>
<td>Risk Assessment</td>
</tr>
<tr>
<td></td>
<td>Sarbox Process Documentation</td>
</tr>
<tr>
<td></td>
<td>Business Plans</td>
</tr>
<tr>
<td>Operating Style</td>
<td>Info &amp; Communication</td>
</tr>
<tr>
<td></td>
<td>IT General Controls</td>
</tr>
<tr>
<td></td>
<td>Division Reviews</td>
</tr>
<tr>
<td></td>
<td>Accounting &amp; Finance Meetings</td>
</tr>
<tr>
<td>Organizational Structure</td>
<td>Monitoring</td>
</tr>
<tr>
<td></td>
<td>Internal Audit function</td>
</tr>
<tr>
<td></td>
<td>IRS audits</td>
</tr>
<tr>
<td></td>
<td>Regulatory Audits</td>
</tr>
<tr>
<td></td>
<td>SEC comments</td>
</tr>
<tr>
<td></td>
<td>SOX Steering Committee</td>
</tr>
</tbody>
</table>

Entity-Level Controls

Entity-level controls are the bottom layer of the wedding cake in the diagram on the previous pages because they are the foundation upon which business processes and other controls rest. Because they are the foundation, the auditor should document them first. The list above shows some of the elements that the auditor must consider at the entity level. The COSO Small Business Guidance contains a good list of the issues that the auditor must cover when documenting the entity-level control section in a SOX 404 project at a small company. The list even includes examples with indications of how to document entity-level processes. The auditor can modify the list to fit nearly any company, saving a great deal of time and avoiding the need to start from scratch.
Entity-Level Controls Documentation

III. Entity-Wide Controls


Entity-Level Controls – COSO Small Business Guidance

The page excerpt above (from the COSO Small Business Guidance) shows an example of the COSO list of entity-level controls. Within the control environment, there are many sections, and this represents an example of the first section: integrity and ethical values. The objective: top management must act ethically and must have a set of standards of conduct for financial reporting. The auditor must examine the following piece of the objective: has management developed a clearly articulated statement of ethical values that is understood at all levels of the organization? The company should achieve this goal. The risk is the inverse of this objective; the company does not have a clear statement of values. The controls are the employee handbook, which contains the ethical values, and quarterly meetings, in which the CEO reinforces these values with upper management personnel.

To test these controls, the auditor must select an appropriate sample of employees based upon the company population size and ensure that members of the sample received a copy of the handbook. Alternatively, the auditor can check signed employment agreements stating that a given employee received and understood the handbook or completed training that covered the company values. The auditor can test the quarterly meeting by examining the meeting agenda and listed attendees, or perhaps electronic meeting notices. The auditor’s goal is to verify that these controls are actually in place; do employees have the handbook, and do the quarterly meetings take place? Auditors using the COSO Small Business Guidance can take the examples from the book as blueprints for the documentation procedures concerning entity-level controls and adapt them to the given company.
Chapter 3 Section 1 – Analysis of Risks and Controls

Entity-Level Controls Exercise

The framework above was again taken from the COSO Small Business Guidance, vol. 3. If the auditor is examining Authority and Responsibility at the entity-level, sub-points 6.1-6.4 identify some questions to ask. For example, 6.1 asks, “Does the Board of Directors oversee management’s process for defining responsibilities for key financial reporting roles?” Sub-point 6.2 asks, “Are the CEO and senior management responsible for sound internal control over financial reporting, including both initiating and maintaining the program?”

The reader should think about the procedures in place at his own company. The next page shows a sample of responses to these questions, also given by COSO.
Entity-Level Controls Exercise: Possible Responses

This chart represents potential responses to the questions posed about the entity-level controls on Authority and Responsibility. A response to the question in sub-point 6.1 is, “Annually, the board reviews authorities delegated to management and management’s process for delineating roles and responsibilities for financial reporting. This is referenced in the board minutes.” A sample answer to the question in sub-point 6.2, is, “the formal job descriptions of the CEO and senior management include responsibility for sound internal control over financial reporting. The board reviews job descriptions annually. This is referenced in the board minutes.” The company does not have to have implemented all of the above controls, as long as it has taken action to address the overall objective: communicating effective control and responsibility over financial reporting.

<table>
<thead>
<tr>
<th>Sub-point</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>Annually the board reviews authorities delegated to management and management’s process for delineating roles and responsibilities for financial reporting. This is referenced in the board minutes.</td>
</tr>
<tr>
<td>6.2</td>
<td>The formal job description for the CEO and senior management include responsibility for sound internal control over financial reporting. Job descriptions are reviewed annually by the board. This is referenced in the board minutes.</td>
</tr>
<tr>
<td>6.3</td>
<td>Formal job descriptions for senior and functional management include responsibility for ensuring that all employees understand the importance of complying with internal control objectives. The organizational chart and job descriptions describe the responsibilities of finance and accounting officers. Organization charts are reviewed annually by the board. This is referenced in the board minutes.</td>
</tr>
<tr>
<td>6.4</td>
<td>Company level policies set limits on who has what approval authority, including the level of transaction requiring board approval. This is re-communicated each year to staff.</td>
</tr>
</tbody>
</table>

## Entity-Level Controls Exercise

<table>
<thead>
<tr>
<th>Principal and Attribute</th>
<th>Controls</th>
<th>Tests</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authority and Responsibility — Management and employees are assigned appropriate levels of authority and responsibility to facilitate effective internal control over financial reporting.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>6.1</strong> Does the board of directors oversee management’s process for defining responsibilities for key financial reporting roles?</td>
<td>Annually the board reviews authorities delegated to the CFO.</td>
<td>Obtain the BoD minutes where the BoD delegates authority to the CFO and CEO.</td>
</tr>
<tr>
<td></td>
<td>The BoD also delegates signature authority to the CEO who in turn delegates to lower management levels. The CEO approves signature authorities.</td>
<td>Obtain the signature lists approved by the CEO. Use selections from testing performed at section LSC-8 (IT testing) to ensure that terminated employees are removed from signature lists promptly. Check for CEO signature on those lists.</td>
</tr>
</tbody>
</table>
| **6.2** Are the CEO and senior management responsible for sound internal control over financial reporting, including both initiating and maintaining the program? | On a quarterly basis, the CEO and CFO report to the audit committee on the quality of the organization’s controls and accounting policies. In addition, all matters of financial importance are raised at the Officer Disclosure and Control Meeting by the Managers of each Department and the CFO. The minutes of the Officer Disclosure and Control Meeting are reviewed by the Committee. The minutes of the Committee are reviewed by the Audit Committee at a special meeting prior to the release of the 10Q or (10K). The Committee minutes are also approved by the full BoD. | Include in the workpapers, the minutes of the following meetings during the year:  
- Quarterly control and Procedure Report  
- Committee Meeting where the Officer Disclosure and Control finding are approved  
- BoD where the minutes of the Committee minutes are approved. |
| **6.3** Are senior and functional management responsible for ensuring all employees understand their responsibilities for achieving financial reporting objectives through adherence to internal control policies and procedures? | | |
| **6.4** Does the assignment of authority and responsibility include appropriate limitations? | See section 6.1 above. | See section 6.1 above. |
Entity-Level Control Exercise: Sample

The chart above represents the entity-level process, “Authority and Responsibility,” for a company, complete with controls and tests. The first column lists objectives; the second column lists controls that the company has implemented; and the third column lists tests for the given controls. The top row asks, “Does the Board of Directors oversee management’s process for defining responsibilities for key financial roles?” This is question 6.1 from the COSO Small Business Guidance example. This particular company has two controls for this objective. Annually the board reviews authorities delegated by the CFO. Also, the Board of Directors delegates signature authority to the CEO and then the CEO gives out signature authority to management. To test the first control, board review of authorities delegated by the CFO, the auditor examined minutes from board meetings to ensure that they included a section about delegating authority to the CFO and CEO. Secondly, the auditor verified the existence of a signature list and that the CFO approved signature authorities. Later, as part of the IT testing, the auditor verified that employees who had been terminated were removed from the signature list.

To summarize the above exercise, examining these company-level controls is the first step in the COSO Small Business Guidance recommendation. It is important that the auditor start at the entity-level because having a strong understanding of the company-level controls will help him learn about possible controls to use when examining the business processes. For example, the auditor already knows about the signature list and who is on it. By the time the audit moves to the expenditure cycle, the auditor already has a good idea of the context in which that cycle takes place.

Starting with the big picture and getting progressively more detailed is an important part of planning documentation procedures. Auditors often want to jump right into documentation, but careful planning up front can save time later. More concretely, starting at the entity-level can save the auditor a lot of effort and expense when the project gets down to the business process level.

For example, one area where entity-level controls are important at the process level might be that the CEO and the CFO always approve expenditures over a certain dollar amount, $25,000. When the auditor is then trying to figure out who must sign a check for $75,000, he already has that information.
Chapter 3:  
Section 1 Analysis of Risks and Controls 

Part 2: Business Process Flowcharts
Examples of 404 Documentation

Examples of 404 Documentation

For Each Process
– Flowchart (or Narrative)
– Risks and Controls Matrix

Business Process Flowcharts

What documentation must the project team create for each business process? Having completed the steps at the bottom of the “wedding cake,” the entity-level controls and IT General Controls, the auditor moves on to business processes. For each process, the auditor must create a flowchart, or narrative. Narratives can effectively document processes, but flowcharts are easier to maintain, easier to understand, and easier for the project team to walk through. The auditor must also create a risk and control matrix. Many times companies will document processes with flowcharts but will neglect the important step of developing risk and control matrices. Creating risk and control matrices establishes a logical system for identifying all the potential risks that could affect the process and the controls implemented to avoid those risks.

Some companies choose not to create separate flowcharts and risk and control matrices, instead writing a narrative about the process and emphasizing risks and controls in boldface type or by underlining them. However, flowcharts, as covered here, are a best practice for documentation procedures.

Microsoft Visio®

– $180 on Amazon.com
– Do NOT buy Visio Professional. It’s $440.
– Do not try to do flowcharts in PowerPoint.

Software Tools for Building Flowcharts

If the reader is not familiar with Visio, it comes in two versions, standard and professional. The standard version contains all of the necessary functions and costs $260 less than the professional version. The 2007 edition is also available and costs slightly more than the 2003 edition pictured here. Building flowcharts in PowerPoint is much more difficult, and Visio offers even the novice the ability to make high quality flowcharts.
Chapter 3 Section 1 – Analysis of Risks and Controls

Hypothetical ‘Swim-lane’ Flowchart

The Swim-Lane Flowchart

Imagine a swimming race at the Olympics; each swimmer must stay in his lane. The same principle governs the swim-lane flowchart. The left-most column lists position titles, and each employee “stays in his lane.” The “lanes,” rows on the chart, show each position’s tasks for the given process. Swim-lane flowcharts work well because they allow the auditor to account for information and communication, aspects of the COSO requirements that companies usually do not address directly. The vertical arrows show communication, information passing between two employees.

This chart shows key controls in the numbered circles. According to the new guidance, the auditor is only required to identify key controls.

The Act requires documenting the process and the point in the process where the control occurs. Two more reasons to use swim-lane flowcharts is that they allow the auditor to visualize exactly where a control is implemented and that it occurs in multiple places.

Lastly, swim-lane flowcharts are an excellent way to show the segregation of duties. The auditor can simply look across a row to see if one person is doing the majority of the tasks in a process. Further, this type of chart allows the auditor to identify problems, such as when one employee does most of the tasks in a process, but very few of the controls cover the tasks done by that employee. Such a picture signals an issue with the segregation of duties in the given process.
Chapter 3 Section 1 – Analysis of Risks and Controls

Real ‘Swim-lane’ Flowchart

Sample Swim-Lane Flowchart

This is a swim-lane flowchart. It shows what could be an issue with segregation of duties. The second row shows the accounts payable function, which contains more activities than any other position in this process. More importantly, there are quite a few key controls in this function as well. Such a lopsided distribution of duties and controls could signal a problem, and the auditor must note these instances during documentation.

While swim-lane flowcharts simplify the documentation phase of a SOX project, the auditor must still take the time to carefully collect the data to be included on each flowchart. The auditor must conduct rigorous interviews of process owners to accurately describe each activity within the process. Some employees may not be forthcoming with information, while others may simply not understand the documentation procedures and the types of information that they should furnish. As a result, though the product looks clean and simple, the legwork behind it is where the auditor will expend the most effort.
Chapter 3:
Section 2 Risk & Control Matrices

Part 1: The Risk and Control Matrix – Assertions
As noted earlier in the book, there are two main documentation work products: the flowchart and the risk and control matrix. The chart above represents a sample risk and control matrix. Control description, frequency and owner columns listed in the second row are normally shown in a continuous row (the row was split for ease of display). At its most basic, a risk and control matrix includes exactly that, risks and controls, listed side by side. However, in practice, the auditor must also document the characteristics of each control as well. The matrix should include the type of control: manual, IT, or hybrid. The auditor also should note in the matrix whether the control is designed to prevent or detect problems; whether or not it is a monitoring control; and if it is intended to prevent fraud or safeguard assets.

Another crucial element of the risk and control matrix is notation of the frequency at which each control is performed. Later, during the testing phase, this is important because a control that is performed more frequently will have a larger population than one performed only sporadically. For example, a control that is performed daily will have occurred 250 times by the end of the year (given a standard work year). With controls that take place multiple times in a given day, such as the sending out of invoices, the population can...
run well into the thousands. A larger population requires that the auditor take a larger sample too. Clearly, a representative sample of the population of invoices must be much greater than a sample of reserve journal entries (which are completed once each quarter).

Two final pieces of data that the auditor must include in the risk and control matrix are the control number and the name of the control owner. These pieces of information help the auditor efficiently build a flowchart. Knowing the name of the control owner tells the auditor in which swim-lane to place the control. Assigning a control number avoids the necessity of writing out the control in longhand on the flowchart. In addition, if there are changes made to a control, the auditor need only note them on the control matrix, and not in every instance of the control on the flowchart. This way, the auditor only needs to change the flowchart if the company changes the location of the control.

New auditors often ask how to number controls. The easiest practice is to number them in the order they occur within a process. Invariably the company will make changes; it will omit some controls, and move others. Additionally, because the data collection process involves interviewing process owners, who will not always describe their duties in a linear fashion, the auditor may not assign control numbers in the same order in which the controls appear in the process. All of these issues mean that the numbering scheme may not remain in consecutive order, and the easiest way to alert the reader of the work documents is to footnote any omissions or changes to the numbering system. Noting changes is much less time-consuming than renumbering all of the controls in the matrix and on the flowcharts. Also, noting changes will avoid a situation in which the reader thinks that something is missing because a particular control number has been skipped.

**Assertions Determine Risks**

<table>
<thead>
<tr>
<th>Assertion</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Completeness</td>
<td>Transactions missing</td>
</tr>
<tr>
<td>Existence/Occurrence</td>
<td>Assets Exist</td>
</tr>
<tr>
<td></td>
<td>Transaction didn't occur</td>
</tr>
<tr>
<td></td>
<td>Transaction is invalid or premature</td>
</tr>
<tr>
<td></td>
<td>Recorded at the wrong amount</td>
</tr>
<tr>
<td>Rights and Obligations</td>
<td>Company doesn't own its assets</td>
</tr>
<tr>
<td></td>
<td>Company doesn't owe its liabilities</td>
</tr>
<tr>
<td>Valuation/Allocation</td>
<td>Bad estimate</td>
</tr>
<tr>
<td>Presentation/Disclosure</td>
<td>Financial Statement presentation is wrong</td>
</tr>
<tr>
<td></td>
<td>(GAAP)</td>
</tr>
<tr>
<td></td>
<td>Disclosure missing or incorrect</td>
</tr>
</tbody>
</table>
Chapter 3 Section 1 – Analysis of Risks and Controls

Assertions: A Review

Assertions, as defined in chapter 2, are the statements that explain the criteria for correct financial reporting. Taken from the COSO Small Business Guidance, the assertions are: Completeness (C), Existence & Occurrence (EO), Valuation & Allocation (V/A) Rights & Obligations (R&O), and Presentation & Disclosure (P&D). The SAS 106 Assertions are described in more detail in the graph on page 69. If the auditor knows which assertions are relevant to each account, and which processes influence each account, then he can map the relevant assertions to each process.

The assertion defines the risk; for example, if completeness is relevant to a particular process, then the risk is that the process might be incomplete. For instance, in accounts payable, a transaction might be missing from the AP account.

Existence & occurrence (EO) means quite simply that assets exist. For example, a balance sheet item exists and an income statement item is a transaction that exists. If an employee stole money and recorded it as an expense, a valid transaction did not occur. If an employee recorded a transaction too early and the shipment did not come in, a valid transaction did not occur. If an incorrect amount was recorded for a transaction, a valid transaction did not occur either. This last example might seem like a valuation or allocation assertion, but in fact, it comes down to existence, because the proper transaction does not exist (only the incorrect transaction has been recorded). The valuation and allocation assertion only concerns judgments and estimates. Improper calculations on invoices resulting in discrepancies between what was billed and what was paid are problems with existence and occurrence.

Rights & obligations (R&O) is quite easy; a company owns its assets, and it owes its liabilities.

Presentation and disclosure (P&D) is related to compliance with GAAP. Presentation and disclosure is usually a relevant assertion in every process. Perhaps in instances such as getting approval for a purchase order, P&D might not be relevant, but otherwise it usually is. Any time the company applies GL account coding and GL distribution, an employee must record the transaction according to GAAP. Also, a missing footnote disclosure is a problem under P&D.

When mapping assertions to accounts, the auditor should also map assertions to footnotes. Thus, the auditor must include not only the trial balances, but also the amounts from footnote disclosures. It is a good practice to include footnotes from other data sources, such as outstanding stock shares, as well. Then the auditor must map processes to key disclosures too.

To sum up, the auditor should think of the above assertions as questions to ask in order to determine applicable risks.
Chapter 3: Section 2 Risk & Control Matrices

Part 4: Controls
Company-Level Controls that Mitigate Business Process Risk

- CEO and CFO review monthly disaggregated gross margin and operating margin data by division.
- CEO and CFO are required to formally authorize all major disbursements or commitment of company funds.
- CFO reviews monthly all judgmental reserve movements for each division.
- Preparation of reporting package by location that analyzes trends in income and working capital – reviewed by CEO, CFO, and Board.
- Review of disaggregated income statements data versus comparable period in the preceding year.
- Preparation and review of monthly closing checklist at each location that local controllership signs and submits to the CFO.
- In addition, the review of budget-to-actual is an important tool in evaluating the result of financial reporting. Budgets are prepared annually and approved by the Board. The controller is responsible for preparing the budget under the supervision of the CFO and CEO and key personnel from each department, operating and financial, are actively involved in the development of the budget. On a quarterly basis, departmental managers meet to discuss the continued appropriateness of the budget and make adjustments necessary to reflect actual experience and current economic and industry conditions and expectations.
- The controller prepares a budget-to-actual report each month and investigates any unexpected results. The controller’s monthly review of the operating reports from all departments and interaction with personnel from those departments/divisions. In addition, key operating personnel are required to review and assess the budget-to-actual report and comment on variances. The completion of the budget-to-actual review requires the approval of all senior management. The integrated nature of the review effectively allows for the timely identification of differences and inconsistencies that may have financial reporting implications.


Company-Level Controls and Business Process Risks

Before jumping into controls, it is a good idea to look at the list above, taken from the COSO Small Business Guidance, as it can help the auditor to avoid some detail work at the process level. The first company-level control is “CEO or CFO review of gross margin or gross margin percent;” this can reveal potential problems if the review is sensitive enough to reveal significant deficiencies. Following the earlier example where materiality was $1 million, the review must be able to pick up a variance of $200,000 over the course of a year.
The next company-level control is “the CEO and CFO should be required to formally approve any major commitment of company funds.” With a select group signing off on any major disbursement, this control mitigates a great deal of risk, unless a member of that group is both requesting and signing off on a given purchase.

“The CFO reviews all judgmental reserve movements each month.” If for example, the auditor is examining the journal entry process, he wants to ensure that one employee prepares the entry and a different employee approves and posts it. Ideally, the preparer and the employee posting the entry should be separate so that the person approving the entry can check to see that it has been properly prepared. However, the auditor would not have to check for this separation if he already knew that the CFO reviews all judgmental reserves as they appear in the financial statements each month. The other theory behind relying on this company-level control rather than checking up on the process itself is that it is best to focus on the controls completed closest to the release of the financial statements. This allows less time between the control and the financial statement during which something could go wrong.

“Monthly closing checklists from each location should be reviewed and signed by the local controller before submission to the CFO.” The review should include prior year vs. current year, budget vs. actual, and other standard checks. If the review is sensitive enough and well documented, the company can use it as an effective control. Such a review allows the auditor to verify that management has approved any differences between the budget and actual numbers.

Having explored a couple of the controls listed in the chart above, the auditor can get a sense of the potential time savings in using entity-level controls to mitigate risks at the business process level.

Best Choices for Controls

- The control must be working.
- There should be some evidence that the control is working.
- The control must be sensitive enough to prevent or detect the risk (error).
- Easy to test
  - Automated (IT) controls are best.
- Control mitigates many risks.
  - Entity-level controls are best.

Seeking Out the Best Controls

Having identified the controls on a given process, the auditor must decide which controls to use. While it may seem obvious, the first criterion is that the control should actually work. After walking through a test with company management, the auditor may find that the process owner does not know how the given process actually works in practice. The auditor has interviewed management to understand and document the
process, but then, when reviewing the process with the employees involved in the transactions, he finds that the practical reality is different. For this reason, the auditor should always verify information learned through interviews with a first-hand look at how the control works. It is essential to have evidence proving that a control is functioning properly. If the auditor cannot find any evidence that the control works, he should definitely not rely upon that control.

Auditors new to SOX projects often ask how to identify evidence that company-level controls are functioning. Even though they are high-level controls, the auditor still must have evidence that company-level controls are working. For instance, the auditor should find written evidence that an employee conducted a budget vs. actual review if that is part of the control. The review should include a note, or a separate document, explaining any variance. Additionally, the auditor should find evidence that the variance has been resolved. The reviewer should have evidence of sending an email or a memo, and of receiving a response.

Another great top-level control is a Management Discussion & Analysis of Financial Condition and Results of Operations (MD&A). Often when companies write MD&As, they do an analytical review to understand fluctuations and variances in relation to the prior year. Again, this can save time if the MD&A process is well documented.

As mentioned earlier, when choosing controls, the auditor must verify that a given control is sensitive enough to actually prevent or detect the risk that it is designed to control.

Also important to choosing controls is that they should be easy to test. For this reason, IT application controls (also known as automated controls) are great; the auditor need only test them once to verify that they are working. With IT controls, the auditor can also apply the concept of benchmarking, which means that if an IT application is working, and its function is verified any time it is changed or upgraded, it need not be tested every year (chapter 5 covers benchmarking in more detail). The principle behind this is that the control over the change verified the application, so it does not need retesting by the auditor. It is not good practice to avoid retesting for too long, but benchmarking allows the auditor to reduce the amount of testing for automated controls.

The auditor should also look for controls that mitigate more than one risk. This makes testing easier.

An important term to know is key control. A key control is not necessarily the only control preventing a risk, but it is the one upon which the company relies to prevent that particular risk. For instance, in the expenditure process, a company might have a variety of controls including, reviewing checks that have cleared the bank when they return with the bank statement, ensuring that an executive not involved in processing the payment signed the check, or ensuring that the person requesting the check was not the same person approving it. However, the auditor may decide that having a management signature on all checks is enough assurance that the process is working properly. The management signature becomes the key control, and the others are secondary controls. The new guidance only requires the auditor to document and test key controls.
Chapter 3:
Section 2 Risk & Control Matrices

Part 5: Creating an Expenditures Risk & Control Matrix
Create Expenditures Risk & Control Matrix

The chart above shows an assertion of existence and occurrence (E/O) for the vendor setup process. Because it occurs early in the expenditure cycle, vendor setup includes only one assertion. The chart shows vendor setup on three different lines, meaning that there are three objectives or controls, or that the company has identified three relevant risks. Conceptually, the auditor then thinks about what could go wrong with vendor setup from the perspective of the existence and occurrence assertion. Perhaps non-existent vendors are listed; an employee, not wanting to raise suspicion, uses an existing vendor but changes the address to a PO box. The employee could then potentially steal any payments made to that vendor. This is one possible scenario.

The auditor could control the vendor setup process at several different points. He could place a control on the addition of new vendors. He could also place a control on changing vendor addresses. Annual, semi-annual, or quarterly review of the existing vendor list is another potential control.
### Risk and Control Matrix

<table>
<thead>
<tr>
<th>Risk Code</th>
<th>Risk Description</th>
<th>Key</th>
<th>Control Type</th>
<th>Prevent/Select</th>
<th>Monitoring</th>
<th>Fraud</th>
<th>Safeguarding</th>
<th>Control Code</th>
<th>Control Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Invalid vendors added to file</td>
<td>Fraudulent or invalid changes are made to vendors in the vendor master file.</td>
<td>K</td>
<td>Manual</td>
<td>P</td>
<td>F</td>
<td>S</td>
<td></td>
<td>EXP-01 AP verifies vendors are approved</td>
<td>Accounts Payable verifies that all invoices from new vendors are approved for validity prior to adding the vendor to the vendor master file.</td>
</tr>
<tr>
<td>Risk Invalid vendors added to file</td>
<td>Fraudulent or invalid changes are made to vendors in the vendor master file.</td>
<td>K</td>
<td>Manual</td>
<td>D</td>
<td>M</td>
<td>F</td>
<td>S</td>
<td>EXP-02 Approval of Checks</td>
<td>Check signers verify the invoice is valid, and the check amount and GL coding are accurate prior to signing the check.</td>
</tr>
<tr>
<td>Risk Invalid Vendors not detected</td>
<td>Inappropriate or inaccurate changes and/or additions to the vendor master file are not detected in a timely manner.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk AP subledger doesn’t close completely to GL</td>
<td>Payables do not transfer completely to the general ledger.</td>
<td>K</td>
<td>System</td>
<td>P</td>
<td></td>
<td></td>
<td></td>
<td>EXP-17 Unbalanced batch will not post</td>
<td>GL System will not post a batch from AP System if the batch is out of balance.</td>
</tr>
<tr>
<td>Risk AP subledger doesn’t close completely to GL</td>
<td>Payables do not transfer completely to the general ledger.</td>
<td>K</td>
<td>System</td>
<td>P</td>
<td></td>
<td></td>
<td></td>
<td>EXP-03 Interface is complete</td>
<td>After each upload from AP System to GL System, Accounts Payable enters the batch total from the AP System Transaction Report into GL System and GL System will prompt if the control total does not match the batch.</td>
</tr>
</tbody>
</table>

### Creating an Expenditures Risk & Control Matrix continued

The chart above represents the same matrix shown on the previous page, with sample objectives, risks, and controls filled in. The first objective is that the vendors are valid, and the second objective is that the vendor list remains valid. Associated with these two objectives are two risks: that invalid vendors are added to the list, or that invalid vendors are not detected on the list of existing vendors. The “K” in the column to the right of the risk description means that the given control is a key control. According to the COSO Small Business Guidance, these are the only controls that must be documented and tested.
## Creating an Expenditures Risk & Control Matrix

This chart displays additional information pertaining to the controls in the vendor setup process (continuing from the illustration on the previous page). The first control was “accounts payable verifies that all invoices from new vendors are approved for validity prior to adding the vendor to the vendor master file.”

The second control was “check signers verify that the invoice is valid and the check amount and GL coding are accurate prior to signing the check.” For this control, the auditor must locate a list of employees authorized to sign checks. The list is not shown on the chart above, but the auditor should attach it as a separate document. The auditor should identify these employees so that he can locate them during the testing phase of the project (in an actual project, they would be identified by name as well as by title). If no one other than the authorized employees can issue a signed check and have it recorded on the books, the company has a very effective control for this risk. The company then relies heavily on these independent employees signing checks.

The last risk, that the existing vendor file could be changed, has no control; there is no one outside of accounts payable who independently reviews the vendor list on a regular basis. This is a design deficiency, and the auditor must document it. Chapter 4 describes a method for documenting design deficiencies.

<table>
<thead>
<tr>
<th>Risk Code</th>
<th>Risk Description</th>
<th>Key</th>
<th>Control Type</th>
<th>Prevent/Detect</th>
<th>Monitoring</th>
<th>Fraud</th>
<th>Safeguarding</th>
<th>Control Code</th>
<th>Control Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk invalid vendors added to file</td>
<td>Fraudulent or invalid changes are made to vendors in the vendor master file.</td>
<td>K</td>
<td>Manual</td>
<td>P</td>
<td>F</td>
<td>S</td>
<td>EXP-01 AP verifies vendors are approved</td>
<td>Accounts Payable verifies that all invoices from new vendors are approved for validity prior to adding the vendor to the vendor master file.</td>
<td></td>
</tr>
<tr>
<td>Risk invalid vendors added to file</td>
<td>Fraudulent or invalid changes are made to vendors in the vendor master file.</td>
<td>K</td>
<td>Manual</td>
<td>D</td>
<td>M</td>
<td>F</td>
<td>S</td>
<td>EXP-02 Approval of Checks</td>
<td>Check signers verify the invoice is valid, and the check amount and GL coding are accurate prior to signing the check.</td>
</tr>
<tr>
<td>Risk invalid Vendors not detected</td>
<td>Inappropriate or inaccurate changes and/or additions to the vendor master file are not detected in a timely manner.</td>
<td>K</td>
<td>Manual</td>
<td>D</td>
<td>M</td>
<td>F</td>
<td>S</td>
<td>EXP-01 AP verifies vendors are approved</td>
<td>Accounts Payable verifies that all invoices from new vendors are approved for validity prior to adding the vendor to the vendor master file.</td>
</tr>
<tr>
<td>Risk AP subledger doesn’t close completely to GL</td>
<td>Payables do not transfer completely to the general ledger.</td>
<td>K</td>
<td>System</td>
<td>P</td>
<td></td>
<td></td>
<td></td>
<td>EXP-17 Unbalanced batch will not post</td>
<td>GL System will not post a batch from AP System if the batch is out of balance.</td>
</tr>
<tr>
<td>Risk AP subledger doesn’t close completely to GL</td>
<td>Payables do not transfer completely to the general ledger.</td>
<td>K</td>
<td>System</td>
<td>P</td>
<td></td>
<td></td>
<td></td>
<td>EXP-03 Interface is complete</td>
<td>After each upload from AP System to GL System, Accounts Payable enters the batch total from the AP System Transaction Report into GL System and GL System will prompt if the control total does not match the batch.</td>
</tr>
</tbody>
</table>
Creating an Expenditures Risk & Control Matrix continued

Shown above is a portion of a flowchart documenting the expenditure cycle described in the risk and control matrix on the previous pages (See Appendix C for the full chart). To understand where the first control (verification that the vendor is valid – control number EXP-01) takes place, the auditor looks to the accounts payable swim-lane. The auditor can check to see how the control verifies that a particular vendor exists. If the vendor does not exist, A/P enters a new vendor, making sure that the invoice is already signed. If the invoice is signed with the proper signature, A/P has implicit approval to enter the new vendor into the list. On the flowchart, the control number (EXP-01) is listed in a small circle next to “setup new vendor in A/P system.” The auditor can look at the risk and control matrix to find information about the control represented by the given number.

The third swim-lane from the top of the flowchart shows the second control discussed on the previous page, “check signers verify that the invoice is valid and the check amount and GL coding are accurate prior to signing the check,” next to the box labeled “Verify Validity, Accounts, Amounts, and Sign Checks” (control number EXP-02).

Thus, by looking at both the risk & control matrix and the process flowchart, the auditor can see the risks associated with a process, the controls implemented to prevent those risks, and the location within the process where those controls take place along with the employees responsible for the control.
Chapter 4: Writing and Implementing Test Plans

Part 1: Inherent Process Risk and Risk of Control Failure
Inherent Risk vs. Risk of Control Failure

The chart above represents the project hierarchy discussed in chapter 2. The light blue boxes above show elements of this hierarchy not explored earlier. Included in the new standard are two types of risk: inherent process risk and risk of control failure. The chart shows inherent risks in the light blue boxes to the right of processes and risks of control failure to the right of controls. In both cases, materiality is separated from risks.

If for example a company installed a new accounts payable system, that new AP module would create inherent risks. Also, the auditor must consider the amount of materiality flowing through this process in order to evaluate the importance of this particular process in relation to other processes.

On the other hand, if the control on this process has failed in the past, or if new employees are responsible for the control, the process itself is not necessarily risky, but risk of control failure is high. High inherent risk combined with high risk of control failure compounds the situation in a given process.

The next few pages describe a method for building a checklist to help the auditor evaluate both types of risk at the same time.
Risk Evaluation Checklist: Inherent Risks

The first step to building a risk detection checklist is identifying inherent risks. The first factor in identifying inherent process risks is susceptibility to errors or fraud. For example, a process involving wire transfers or cash is susceptible to fraud. If a company pays its vendors in cash, the fact that the company must keep large sums of cash on hand makes this process highly susceptible to fraud.

The second risk factor is complex accounting (GAAP). Processes involving derivative instruments require that a company comply with the 200+ pages of FAS 133, making it very easy for employees to make mistakes simply due to the complexity of the procedures. Taxes are another area that hurt companies during the early years of Sarbanes-Oxley. Many companies have complicated tax issues, including short-term and long-term deferred taxes, deferred tax assets and liabilities, tax provisions and tax contingencies.

A third set of inherent risks comes from processes that involve subjectivity, estimates and judgments, contingencies, reserves, impairments, and intangible assets.

A fourth risk factor is the complexity of transactions involved in a process. Even if GAAP is not complex, some processes contain complex transactions. A company might have several distribution layers in its sales process. The salesperson sells to an agent, who then holds inventory and sells to distributors. There is also a great deal of complexity in revenue recognition, where the many rules about who holds the title, who paid for the shipment, who bears the risk of loss, and who has the right of return, can create a more risky process.

Lack of automation is the fifth risk factor. The more IT controls a company has, the greater the certainty that a process will be completed correctly every time it takes place. However, one important caveat to this factor is that spreadsheets increase risk.

Chapter 3 also identified changes to processes as points where risks can develop.
Chapter 4 – Test Plans

Contingent liabilities, another risk factor, are similar to subjectivity and estimates.

Related party transactions also increase the possibility of risk because of potential conflicts of interest. For example, the president of the company leasing space or equipment to the company is inherently risky.

Lastly, environmental factors such as technological or economic developments can increase risk as well. For example, a bank with processes involving interest rate changes or exposure to sub-prime mortgages has high risk factors.

This chapter covers a format for evaluating these risk factors a bit later, but these are the problem areas to which the auditor should pay close attention when examining processes.

Risk of Control Failure

Risk of Control Failure
- The nature and materiality of misstatements that the control is intended to prevent or detect;
- The risk of management override;
- Whether there have been changes in the volume or nature of transactions that might adversely affect control design or operating effectiveness;
- Whether the account has a history of errors;
- The effectiveness of company-level controls, especially controls that monitor other controls;
- The degree to which the control relies on the effectiveness of other controls (e.g., the control environment or information technology general controls);
- The competence of the personnel who perform the control or monitor its performance and whether there have been changes in key personnel who perform the control or monitor its performance;
- Whether the control relies on performance by an individual or is automated (i.e., an automated control would generally be expected to be lower risk if relevant information technology general controls are effective);
- The complexity of the control

Risk Evaluation Checklist: Risk of Control Failure

In addition to inherent process risk factors, there are several signs, shown in the chart above, that point toward risk of control failure. The first is the materiality that the control is preventing. The auditor should not confuse this with the materiality of the process itself.

A second factor is the risk of management override. A company might have a situation in which the treasurer approves wire transfers. If employees working for the treasurer are always subject to the treasurer's approval, management can override any existing controls in the department.

The third factor is a change in volume or nature of the transactions monitored by a particular control. If for instance a company centralizes accounts payable when it had a previous practice of keeping separate A/P processes in each of its locations, the A/P staff at the headquarters now has a much greater volume of work. This increase in workload can lead to mistakes in the application of controls in the process.

The fourth factor, a history of errors within an account, is obvious; if a control failed during previous tests, it may fail again in current tests.
The auditor should think of the fifth factor, effectiveness of company-level controls, as “ineffectiveness of company-level controls and lack of monitoring.” If no executive or internal auditor reviews a particular process, lack of oversight creates a high risk of control failure.

The auditor should also consider the degree to which controls rely upon other controls. For example, a company could rely on the fact that no one can hack into the payroll system to change a salary. This means that the company counts on effective controls on the IT infrastructure. Without knowing that such a hack is impossible, the company cannot be certain that the IT control on fraudulently changing a salary will work properly. In other words, any problems with IT controls on database access raise the risk of using IT controls to secure the payroll.

As mentioned in chapter 3, personnel competence is a factor in the risk of control failure, especially with personnel turnover.

Manual controls also pose a greater risk of control failure than do automated controls. If there are no underlying problems with IT controls, automated controls do not involve as much subjectivity as manual controls. For instance, the A/P module should not let an employee enter the same invoice twice; it should catch the error and alert the employee. On the other hand, relying upon an employee to manually keep track of the invoices that have been paid and those that are still outstanding raises the risk of duplicating a payment.

Complexity in performing a control makes it more prone to failure as well. For instance reconciling a liability account of goods received but not invoiced (RNI) is generally more difficult than reconciling a cash account.

Considering these factors points the auditor toward risks of control failure. These are separate concerns from inherent process risks, and the project must account for both types of risks according to the new auditing standard.
The new SOX guidance includes the concept of the heat sheet. The idea behind the heat sheet is that higher inherent process risk (shown in the chart as Misstatement Risk of Financial Reporting Element), coupled with higher risk of control failure, indicates a need for more rigorous testing. In such a case, the auditor should gather more evidence and test larger samples. The opposite is true as well. If a process has a low inherent risk and a low risk of control failure, the auditor can save time and effort by reducing the amount of testing done. The heat sheet diagram is a nice graphical tool that helps the auditor represent the relationship between risks and necessary level of testing.
Chapter 4:
Writing and Implementing Test Plans

Part 2: A Risk Based Approach to Testing
Chapter 4 –

Test Plans

Risk-Based Approach to Testing

Evaluating Inherent Risk and Risk of Control Failure

Knowing the risk factors discussed on the previous pages, the auditor can then develop a spreadsheet like the one pictured above (the image above is cropped – appendix C shows the full spreadsheet). This chart can be used to show the inherent risk factors as well as the factors in risk of control failure. The auditor assigns a specific weight to each of the factors; this assignment process must be linked to the importance of each factor in the structure of the company under review. First, this chart shows that total inherent risk and total risk of control failure have been weighted equally, and account for 50% of the overall risk. Materiality at the process level accounts for half of the weight assigned to inherent process risk. The other half of the weight assigned to inherent process risk is divided among the other factors as shown.
Evaluating Inherent Risk and Risk of Control Failure

The chart above shows the risk of control failure section of the risk evaluation spreadsheet. The full spreadsheet can be found in Appendix C, where the reader can see how this section fits with the inherent risk section discussed on the previous page. The reader should note that because there can be multiple controls for any given process, the inherent risk factors are evaluated in relation to the process itself, while the factors contributing to risk of control failure are evaluated in relation to particular controls. For this reason, the left-hand column of the full spreadsheet shows a process name with control names indented below it, indicating controls associated with a specific process. The auditor assigns weights to each risk of control failure similarly to the procedure he followed with inherent process risks.

Once the auditor has developed a spreadsheet and assigned weights to each factor, he then evaluates each risk factor, typically on a scale from one (1) to five (5), with 1 indicating a low risk and 5 indicating a high risk. As an example, if the auditor were to fill this spreadsheet out for the vendor setup process, few cycles would have a greater material impact upon the financial statement than expenditures (except perhaps revenue or payroll). A bank might have low expenditures, as its primary needs are furniture and office supplies. On the other hand, most companies, especially manufacturing companies, will have sizable expenditures, as they must purchase raw materials and production equipment. As a result, the auditor can assign a rank of 5 to materiality, in the first column of inherent risk factors, denoting a high risk.

Vendor setup contains no serious risks of susceptibility to errors or fraud, but the sample company does not seem to have good control over the process, as they do not review the vendor list. Considering this lack of control, the auditor could mark this as 4, an above average risk.

Complex accounting is probably not a factor in vendor setup, so the auditor might only rank that 1, a low risk. Subjectivity, estimates, and judgments are not likely to enter into vendor setup either so the auditor can assign a low risk (1) here as well. The auditor might decide that transaction complexity is a little higher risk (2), since most transactions are simple, but some are not. Since signatures are involved and the company adds vendors manually, lack of automation is a fairly high risk (4). If no recent changes have been made, the auditor can rank change as a low risk (1). As contingent liabilities are probably not a factor in A/P, they pose a low risk as well (1). A smaller company might have more related-party transactions, making this a higher risk (4). Technological developments are probably a low risk (1) too.
Having made judgments about all of the inherent risks in the vendor setup process, the auditor must assess the risk of control failure. Again, while he evaluates inherent risk factors in relation to the whole process, the auditor must consider factors in risk of control failure for each control within the process. The second and stronger control identified earlier for the vendor setup process, EXP-02, is a good example. This control states, “the check signers verify that the invoice was valid and the check amount and the GL coding are accurate prior to signing the check.” Here again, as with the process itself, materiality is a high risk (5) since this control covers many large transactions. Risk of management override is also a high risk (5) since there are seven employees authorized to sign checks, and they might instruct accounts payable to process a particular invoice. Because the example showed little change in volume, this risk associated with change is lower than average (2). As control EXP-02 has no history of errors, the auditor can rank this risk as low (1).

When the auditor evaluates the effectiveness of company-level controls, the importance of starting the project at the entity-level becomes more apparent. Because the sample company had implemented an executive signature approval process and had management review the financial statements, this risk is fairly low (2). In other words, the company has strong entity-level controls.

This particular control does not rely upon other controls, so reliance on the effectiveness of other controls is a low risk (1). Since the employees performing this control are executives (those authorized to sign checks), the auditor can infer that they are competent, making this a low risk (1) as well. No changes to the process or personnel create a low risk factor (1) too. Again, the auditor can better understand many of these factors with a thorough entity-level interview at the start of the project.

Control EXP-02 is a manual control, not an automated one, so it has a higher risk (4), but the control itself is fairly simple, lowering the risk of failure (1).

Using the weighted contributions of both inherent process risks and risks of control failure, the auditor can calculate a composite risk for each control in the process (a number between 1 and 5 given the scale used in this example). The difficult element here is deciding what composite scores constitute high, medium, or low risks according to the heat sheet. If the score for the sample judgments made above was 3.7, does the auditor consider this a medium risk, or a high risk? The auditor must make a judgment as to the range for a medium risk. It could be any score between 2.5 and 3.5, between 2 and 4, or any other range, but ultimately, the same range should be used for every control in the project. If for the sake of argument, the auditor determines that a low risk is any score below 2, a medium risk is any score between 2 and 4, and a high risk is any score above 4, then the sample control has a medium risk. During the testing phase, the auditor should gather evidence and take samples according to the criteria set up for a medium risk.

Coming up with a concrete method for determining the level of risk for each control is essential because the auditor must be able to show evidence to support judgments about the levels of risk involved in each process and in each control. Earlier in SOX history, verifying level of risk was not necessary, but the new standard is more rigorous in this area. To further document the judgments made in the risk factor evaluation, the auditor can add comments to each ranking, indicating why a particular factor was rated high or low.

Additionally, the project manager should review the development of the risk analysis spreadsheet with the external auditor early in the project. It is not necessary to review the composite scores for each process and its associated controls, but it is a good idea to go over the framework with the external auditor. Also, the project manager should discuss the determination of ranges for high, medium, and low risks with the external auditor. A good way to decide on these ranges is to meet with the steering committee to explore what the scores mean and how sensitively testing should be done. Usually the external auditor will provisionally accept the ranges, and ask to see the composite scores once the project team has calculated them for the whole project. Upon looking over the scores, the external auditor may suggest some adjustments to the ranges, but if this is done before starting the testing phase, the project team can avoid having to start over, gathering new evidence and samples for the affected tests.

New auditors often ask if risk factors are the same for every cycle and set of controls. The lists shown on pages 114-116 were developed by COSO as part of the new standard, and apply to all processes and controls to determine both levels of inherent risk and risk of control failure. Also, SOX does not require auditors to evaluate processes and controls in the quantitative manner described here. Some companies take a simpler approach and consider all controls low risk at the start of the evaluation. If the auditor finds inherent process risk factors and risks of control failure, he raises the risk from low to medium or to high. For instance, companies may decide that related-party activity in a process automatically indicates a high risk, regardless of the presence or absence of any other factors.
Despite the need for accurate and detailed documentation of the risk evaluation procedure, the project team should make sure that work papers are simple to understand so that testers do not make errors when applying these ideas during the testing phase. Often a company will have overseas locations where the employees conducting testing might not speak English as their first language. In general, an overly complex risk evaluation procedure runs the risk of confusing testers (English-speaking or not). In sum, the project team should attempt to make the risk evaluation documents as clear as possible.
Determining Standards for Testing

The chart shown above shows another detail from the risk evaluation spreadsheet discussed on the previous pages (see Appendix C for the full chart). Once the auditor has determined a judgment of the risk for a particular process and control, his next step is to develop a testing plan. He will need to select an appropriate level of evidence; monitoring or inquiry might be acceptable for testing a control with a low risk of failure, while observation, examination, or re-performance may be necessary for a control with a higher risk of failure.

Another question the auditor should ask is whether internal employees or external consultants should conduct testing. Keeping in mind that because the billing rate for external consultants on the project team is quite high, the project manager might choose to use peer testing for lower risk controls, saving the consultants for testing more complex, higher risk controls where independence is essential. As mentioned earlier, having the A/P manager test the accounts receivable process and the payroll manager test the A/P process is an example of peer testing.

Determining testing frequency is also important in planning the testing phase. As mentioned in the discussion of Sections 302 and 404, some testing must be done quarterly, while the auditor can perform other tests on an annual basis. The auditor could choose to test controls that earned a high composite risk score in the second, third, and fourth quarters. Again, companies do not conduct much testing in the first quarter since they have just completed year-end certifications. The auditor may confirm test results for high-risk controls every quarter as well. He might test a medium risk control in the third quarter, but confirm test results in the first, second, and fourth quarters. Determining testing frequency is an essential part of budgeting and planning for the testing phase.

Selecting an appropriate sample is important to planning the testing phase and can help meet budget demands as well. Taking a smaller sample, where possible, allows the project team to spend less time on a particular test, thus saving money.

There are two ways to make the important determinations described here. Either the auditor can make judgments about each control individually, or he can set up a formula establishing level of evidence,
Test Plans

frequency, sample size, and internal or external testers. For example, the auditor could write a formula stating that medium-risk controls be tested twice a year, by an external (independent) tester who will gather and examine evidence.

Risk-Based Approach to Testing

Risk-Based Approach to Testing
More evidence for high risk:
- Bigger samples
- More independent testers
- More frequent testing
- Keep evidence separately (binders)

If less risk
- Rely on monitoring, self-assessment
- Knowledge & supervision by management (with some evidence)

Multiple Locations
- High Risk – get more evidence
- Low Risk – self-assessment, monitoring, central controls

Collecting and Storing Evidence

To summarize the risk-based approach to testing, higher risks require bigger samples, independent testers, and more frequent testing. Properly documenting and testing all of the risks involved in a company’s business processes and associated controls requires that the auditor gather a great deal of evidence. The best way to keep track of evidence is to store it separately in binders, one for each cycle (Part four of this chapter discusses binders in more detail). Sometimes, with higher risk processes and controls, the project team will need several binders for a given cycle.

Aside from making the tester’s job easier, putting all of the documentation and testing information in binders organizes it neatly and clearly for the external auditor. If the external auditor had to track down all of the evidence that the project team has just collected, he is unlikely to rely upon their work. At the very least, he will have to expend a great deal of effort to locate the evidence if it is scattered around in various electronic files and if copies of evidence are not readily available. Part three of this chapter explains the advantages of external auditor reliance.
Chapter 4:
Writing and Implementing Test Plans

Part 3: A Risk Based Approach to Testing
II – External Auditor Reliance
External Auditor Testing

Understanding external auditor reliance is a key to efficient SOX testing. While the company can do some testing internally, the external auditor must conduct tests in two important areas. The first such area is IT general controls (ITGC – these fall under IT infrastructure in the “wedding cake” diagram used earlier in the book). The second is financial reporting. Aside from these two areas, the auditor may, at his discretion, rely upon work done internally, according to the new guidance.

How much can the auditor rely upon internal testing? The company’s internal SOX team must always do more work than the external auditor. See an example below.
Chapter 4 –

Test Plans

<table>
<thead>
<tr>
<th>Number of items selected</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td>Weekly Control</td>
</tr>
<tr>
<td>Selected internally</td>
</tr>
<tr>
<td>80% reliance by external auditors</td>
</tr>
<tr>
<td>50% reliance by external auditors</td>
</tr>
</tbody>
</table>

In the illustration above, the reader can see that the more the external auditor can rely upon the internal work, the better. For instance, if the internal SOX team selected 60 items to test daily controls, the external auditor will examine 30, which is half of those same items at 50% reliance. However, the external auditor can justify re-examining just 12 items at 80% reliance.

In the previous illustration, the external auditor is applying their reliance to every internal test. Another way for the external auditor to apply their reliance is to select an entire test instead of specific items within a test. See the illustration below:

<table>
<thead>
<tr>
<th>Test</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td>Weekly</td>
</tr>
<tr>
<td>A B C D E F G H I J</td>
</tr>
</tbody>
</table>

Items selected internally     | 8 8 8 8 8 60 60 60 60 60 |
Tests selected by external auditor at 80% reliance | 8                      |
Tests selected by external auditor at 50% reliance | 8 8 8 60 60 |

In the above example, the external auditor has applied their 80% reliance by re-examining 20% of the tests (2 out of 10 tests). For the 2 tests selected, the auditor looks at all items. For 50% reliance, the external auditor re-examines half of the tests (5 out of 10).

Variables Affecting Auditor Reliance

It is important to emphasize that 80% is the upper end of external auditor reliance. In practice, external auditor reliance could be lower, even 0%.

Achieving 80% reliance requires considering several different elements. First among these elements are competent testers. To verify that the testers are competent, the external auditor will ask for resumes. The testers’ resumes must demonstrate that they have experience with SOX testing or auditing. Additionally, the
testers should have credentials that indicate their familiarity with business processes. Acceptable credentials are certification as an internal auditor (CIA), CPA, management accountant (CMA), several years of experience as an internal auditor, or an MBA. Stronger resumes will help increase reliance.

The next element is the quality of the work itself. It is very important to have neat, well-organized work binders that have been independently reviewed by senior management. To verify the work done, the project team should have the preparer sign and date each work paper. Then, the reviewer should sign and date each paper as well, using a different color of ink. The reviewer will also produce “review notes,” which must then be cleared by the preparer. In short, the work must be done as if it were an actual audit. Strict attention to detail can help raise the level of reliance, saving the company a great deal of money.

The third variable affecting auditor reliance is independence. Here, the composition of the steering committee is important. If the CFO is running the project and presenting materials to the board, the project team cannot claim complete independence. To improve independence, larger companies will have the SOX team report to the Director of Internal Auditing who chairs the steering committee. Having the Director of Internal Auditing report to the board offers greater separation between the project team and company management. Because a SOX project includes many checks on the finance and accounting department, the company runs the risk of having employees suppress a deficiency, or record a material weakness as a significant deficiency. As a result, having an independent channel through which to report to the board can improve reliance.

As mentioned earlier, there are several types of testing: peer testing, self-testing, and third-party testing. One special form of testing pertains to reliance: the situation in which a company uses controls that are actually performed by a third-party contractor. For instance, some companies use web-based GL systems that are hosted by third parties. Other companies use contractors such as Paychex, Inc. and ADP, Inc. for payroll. A company that contracts out its payroll risks the improper calculation of garnishments, vacation accruals, or tax withholding, for which it is liable.

Because it would be impossible for companies such as ADP, Inc. to allow every SOX team to test their controls, the AICPA developed Statement on Auditing Standards #70 (SAS 70). SAS 70 identifies a set of rules for auditing service providers and writing the subsequent report. SAS 70 audits must explain audit procedures and conclusions, noting which controls are functioning properly and which are not. Rather than allowing every client to come test their controls, a company like ADP will have a SAS 70 audit performed, and will make the report available to clients who request it.

ADP’s clients must then read the SAS 70 report to find out exactly what was tested, in order to ensure that the audit meets their own SOX control needs. For example if a company relies upon ADP to calculate vacation accruals, and they were left out of the SAS 70 audit, the company must build in alternative controls to check the number of employees, average pay, and average length of service. As an alternative to relying on the ADP SAS 70 report, an employee within the company could develop a spreadsheet that approximates vacation accrual and compare his results with the ADP calculations. The company continues to use the ADP figures for its vacation accrual, but the internally produced approximation verifies those figures for reasonableness, acting as a control. The project team can then review the reasonableness check as a means of testing.

There are two types of SAS 70 audits; for a SOX project, it is essential to have a “type two” report. “Type one” audits simply document the processes; “type two” audits include testing as well. “Type one” SAS 70 audits do not meet the standards of the Sarbanes-Oxley Act.

It is important to note that SAS 70 audits are very expensive; they can cost hundreds of thousands of dollars. As a result, companies should write into their contracts with vendors that the vendor will obtain a SAS 70 audit should it become necessary. Many third-party vendors do not want to cover the cost of such an audit and will attempt to pass it on to their clients; this practice can greatly increase a SOX project budget.

In addition to third-party service providers, for which the project team should obtain a SAS 70 report, some companies employ expert contractors such as actuaries or investment advisors. For example, a company might hire an actuary to compute a vested benefit that has accrued to that company’s retirees. Despite the fact that the actuary is calculating the benefit and the company is using the resulting numbers, it is not necessary to obtain a SAS 70 report from the actuary. The actuary is considered an expert, and thus his calculations more reliable than those performed by a company employee. When relying upon such an
expert, a company merely needs to verify that person’s credentials and qualifications. The AICPA wrote SAS 73, which defines guidelines for relying upon expert credentials and qualifications.

Along with competence, quality, and independence, the project team must be able to prove that they randomly obtained samples. In the work papers, the project team must describe the population in detail. They must also indicate their method for generating a random number and for applying this number to the population to obtain a sample. This information is essential to improving auditor reliance as it proves that the sample was not biased or taken haphazardly or out of convenience.
Chapter 4:
Writing and Implementing Test Plans

Part 4: A Risk Based Approach to Testing
II – Compiling Work Papers
Building a Work Binder

In the work binder, the auditor should place the risk and control matrices, flowcharts for all of the processes in the cycle, and, as testing progresses, the evidence that is collected. While most of this information will exist in electronic form as well, keeping hard copies together in a binder allows the tester to use it as a portable reference. As previously mentioned, collecting the work papers in a binder also creates a neat package that can be given to external auditors.

Another investment that can greatly facilitate the testing project is a wide format printer. Relatively inexpensive printers that can print on 11x17 pages in color are available. Such a printer permits the auditor to print out entire spreadsheets and flowcharts in a size that is still readable. Printing a complex spreadsheet on letter-sized paper requires condensing the font size, making the text difficult to read. A large format printer is a small expense, but it can save time during the testing phase when testers have to refer repeatedly to the risk and control matrices and flowcharts.

In addition to the risk and control matrices and flowcharts, the auditor will also place the testing documents in the binder. When compiling the binder, the easiest way to organize the material is to insert tabs for each control. The first tab lists all the risks, controls, and tests for the whole cycle; then each subsequent tab divides the binder by control. Then, for each control, the auditor will list all of the items tested and the sample selection procedures. Lastly, the auditor will file copies of all the evidence gathered for that particular control in the given section.

Another simple but important practice is to label the binders with the project manager's or librarian's contact information by stapling a business card to the binder cover sheet. With the amount of effort that goes into compiling these binders, they are very valuable (if external consultants conduct testing, one binder can hold over $10,000 worth of the project team's work), and it is essential that the project team be able to locate a binder easily in the unfortunate situation that one gets lost. Another good way to safeguard the binders is to have the project librarian check them in and out to keep track of who has them and where they are at all times. Because the company is recommended to keep these binders for 7 years, clearly identifying them is critical to the overall review process as well.
The project team also needs to consider the possibility of tracking testing documents from subsidiaries. If the project team does not visit a subsidiary, but instead asks the testers on site to send back the evidence collected, using a parcel service creates a huge risk given the value of the testing binders. To avoid this risk, it is worthwhile to hire temporary employees to scan the testing materials and save them electronically on CDs.

Scanning the testing binders offers the further benefit of simplifying storage of the project documents. Because seven years worth of records must be kept, having access to them on CD makes reviewing previous years’ tests much easier. It also lowers the cost, in terms of both space and money, of storing the testing documents. Over seven years, the company will accumulate hundreds of binders.
Chapter 4 – Test Plans

What is a Walkthrough?

What is a Walkthrough?
- Physical “walk-through” the documented process from beginning to end with the Control Owner
- Observe the steps and controls in the process. Mark hardcopy documentation with discrepancies.
- Observe Physical security.
- Confirm employee’s understanding of controls and the timeliness of performance.
- Confirm what happens (per documentation) when there is an error.
- Identify recent changes in the process.
- Note un-identified risk or controls that are ineffective.
- Obtain copies of testable documents and screen shots that show the documented process.

Conducting a Walkthrough

While SOX does not require an internal project team to conduct a walkthrough, it is a very worthwhile practice. The project team can often learn more about whether or not a control will pass during the walkthrough than during testing. By doing a walkthrough, the team can also identify documentation problems and correct them before collecting samples and testing. If these problems were found during testing, the given tests would have to be redone.

Although internal auditors are not required to conduct walkthroughs, the external auditor must conduct them. However, the external auditor is not required to walk through all branches of the flowchart. For example if a company’s sales are primarily handled by sales agents, but 5% of its sales come from the internet, the auditor will in all likelihood only walk through the transactions completed by the sales agents. If the auditor walks through the process and finds problems, the project team will have to go back and make changes. Finding these problems before the external auditor uncovers them will improve reliance, as the project team will have created more complete, accurate documentation.

Conducting a walkthrough involves physically examining a given process from start to finish, checking to see that the documentation accurately describes the actual practice. The project team should mark any changes on the documentation; if the changes are small, the librarian can make them, but if they are more involved, such as a problem with a control or a segregation of duties issue, the auditor should make the changes and re-evaluate the control.

During the walkthrough, the project team should observe the physical security of the process. For example, if checks are to be kept in a locked drawer, this should be verified. The project team should also ask employees if they understand each control, its intended purpose, and how to implement it.

Walkthroughs can also help the project team find changes in a process. If the team has conducted previous SOX work, they should walk through the processes after the new year starts to identify any changes. Even though process owners submit signed quarterly confirmations to note any changes or to verify that no changes have been made, they can forget, and the project team can identify these changes in a walkthrough.
Chapter 4 –

Test Plans

It is also important to document the walkthrough, because if it is done thoroughly, the external auditor can rely upon it as well. A good way to document the walkthrough is to develop a checklist. The chart above can be made into a checklist, and with a team member’s signature and date at the bottom, it can be effective evidence of a walkthrough upon which the external auditor could rely.

Lastly, while the project team is gaining SOX experience, conducting a walkthrough is a good way to learn to identify the proper populations for testing. The walkthrough can also be an important tool for training new testers. The project manager can collect examples from the walkthrough to show new testers what to test and how to conduct the given tests.
Chapter 4: Writing and Implementing Test Plans

Part 5: A Risk Based Approach to Testing

III – A Test Plan Example
Example Test Plan

Creating a Test Plan

The illustration above shows an example of a test plan created in Excel®. It would be one tab in an Excel® workbook. The first tab of the workbook would contain the testing instructions; the second tab of the workbook would summarize all of the controls and tests, including results for each (whether or not each control passed); the sheet shown above would be the third tab, and would give testing details for a particular control. The project team would also make a hard copy of this tab for every control tested.

As shown above, the top of the tab describes the control, the population, the required sample size, and the testing procedures. The rows below the procedure description identify the items selected. The first few columns identify each selected test item. If for example, the tester is examining journal entries, he can identify them by journal entry number, amount, and date. The next columns describe the attributes to be tested. For example, attributes might include: journal entry approvals must have occurred before the 10-Q report was published, signatures are those of employees approved to sign entries, and the entry has been coded with the proper GL account for its type. Another column will verify that the support attached to each entry (showing the calculation process done in the spreadsheet) matches the amount of the entry. Once the tester has labeled the columns, he fills in the appropriate information for each test item.

Because the criteria differ for each control, it is a good practice to make the test plan sheets in Microsoft Excel® so that they are easy to change; the auditor can add or remove columns, and edit labels as needed.

It is important to make information about the actual risk available to the tester. While the tester is concerned with verifying controls, knowing the risks those controls are intended to prevent is crucial to making judgments about anomalies. For example, if a journal entry required the signature of the accounting manager, and the controller signed one sample entry, a tester unfamiliar with the risk involved might fail that item. However, if the risk is that the preparer of the entry is also the reviewer, as long as the controller is not the one who prepared the entry (a highly unlikely event), the need for an independent review of the entry has still been met. Furthermore, if the controller is the accounting manager’s supervisor, this particular entry has the signature of an even more qualified reviewer than originally required by the control. As a result, if the tester knew what the risk was, he would probably pass this item. The tester would simply note the reason for...
the controller’s signature (perhaps the accounting manager was on vacation or sick), and that the controller was not the one who prepared the entry, thus maintaining the independent review procedure required by the control.

A Sample Test Plan: The Expenditure Cycle

As mentioned above, a test plan Excel workbook for the example expenditure cycle would contain four tabs. Appendix D shows the sheets that would correspond to these four tabs: testing instructions, a summary of all tests to be performed, and one sheet for each of the controls (EXP-01 and EXP-02) identified for the vendor setup process. An actual test plan workbook would contain more than two controls (EXP-01 and EXP-02) per cycle.

The text shown above comes from the first tab of the sample test plan workbook. While the project manager will have already trained the testers, this page serves as a guide to which the tester can refer at any time during the testing process. The first paragraph discusses the types of evidence that the tester can gather. The second paragraph covers differences between types of evidence and the importance of gathering multiple types of evidence. The third paragraph warns the tester of possible problems that should be identified (for a complete instructions sample, see Appendix D).

Exploring an example can give the reader a clearer idea about the need for detailed instructions. If the tester must verify that an independent reviewer signed a journal entry, a better practice is to check for the authorized signature and to review the entry as well. This allows the tester to identify a situation in which the reviewer approved the entry without actually checking the supporting documents. In short, the tester should find out whether or not the reviewer diligently performed the control. If an authorized employee properly signed the journal entry, but the spreadsheet numbers do not match the entry amount, the test item would fail.

Population & Sample Size Guidelines

<table>
<thead>
<tr>
<th>Population &amp; Sample Size Guideline</th>
<th>Define the population</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Determine the appropriate population for the control being tested. Ensure the population is valid.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Select the sample</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sample sizes have been standardized based on the risk of the process/control and the frequency of the performance of the control</td>
</tr>
<tr>
<td>Sample sizes listed below are minimum sample sizes and may be adjusted upwards to reflect the risk of the process/control.</td>
</tr>
</tbody>
</table>

NOTE: In certain situations, the frequency of the performance of the control may not be an adequate indicator of the population size. (Example – a control may be performed monthly but is performed monthly for each employee, invoice, etc. The population size is not 12 and therefore the sample size suggested for a monthly control is not appropriate.) In situations such as this,
determine the population size and determine the appropriate sample size based on the chart below.

![Minimum Sample Sizes by Risk:](image)

Note: Population definition/determination and sample selection must be adequately documented for re-performance.

**A Sample Test Plan: Testing Instructions Continued**

Descriptions of the population and sample are the next elements of the instructions sheet in the test plan workbook. The information above comes from the testing instructions for the expenditure cycle case (see Appendix D for the complete instruction sheet).

The tester must know how to define the population. For example, if testing is to be done in the third quarter, the population should include everything from January 1 through the testing date where possible. The tester should also indicate the name of the employee who supplied the population and what was obtained, including names of reports and as much other identifying information as is possible. This facilitates re-performing the test in subsequent years.

**Control Frequencies**

**A Sample Test Plan: Control Frequencies and Populations**

This chart shows frequencies of some common controls to give the reader a sense of population sizes. Knowing the population size is critical for determining the size of the sample to be tested. For example, a control performed daily such as sub-ledger distribution will have a population size of 250 (based upon a typical work year). On the other hand, an annual control such as a 10K report will have a population of 1.
Control Frequencies / Sample Sizes

**A Sample Test Plan: Determining Sample Size**

The chart above describes sample size and shows an important aspect of the risk-based approach. The risk level involved with a particular process and control determines possible sample size. The project team should discuss sample sizes with the company’s external auditors. As developing a sample size is subject to judgment, deciding upon appropriate sample sizes is another area in which early consultation with the external auditor is essential. If all controls were evaluated as high risks or if no risk assessment were done, the required amount of testing work would be about double that of low-risk controls. Thus, while developing the risk and control matrix takes some time early on, it can significantly reduce the amount of time the project team spends on the testing phase.
Chapter 4 – Test Plans

Sampling Period

A Sample Test Plan: The Sampling Period

Level of risk is part of developing an appropriately sized sample; knowing the sampling period is also important. Typically, the auditor takes a sample from the population that exists between January 1, and the testing date. The important exception to this rule is the implementation of a new control after January 1. In such a case, the auditor must take the sample from the period after the new control was put in place.

Exceptions:

<table>
<thead>
<tr>
<th>Control Frequency</th>
<th>Tolerance</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Many X / Day</td>
<td>1 or more</td>
<td>The tester will need to perform additional analysis and testing to provide statistical support for accepting the test findings as Effective (errors were not statistically significant).</td>
</tr>
<tr>
<td>Daily</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Weekly</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monthly</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Quarterly</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Semi-Annually</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Annually</td>
<td>0</td>
<td>With small sample sizes, any exception leads to control failure.</td>
</tr>
<tr>
<td>System</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Exceptions are instances discovered during the testing process where the control actively in place is either not designed or executed appropriately to mitigate the risk identified. When the control actively is not executed in a manner that is effective in mitigating the identified risk, the tester needs to determine if the situation warrants additional testing.

Finding several errors during the testing of the sample items would indicate a gap and require the development of a remediation plan related to the control activity.

Alternatively, one error may be encountered during the testing and the Testing Resource does not believe the error is representative of normal operations. Additional analysis and testing may provide statistical support for accepting the test findings as Effective (the errors encountered were not statistically significant).
A Sample Test Plan: Testing Instructions Continued

The information shown above is the last element of the instructions included in the test plan workbook (see Appendix D for complete instructions). The above section on exceptions tells the tester what to do if a test item fails. If the sample size is large, the tester may accept one failed item, but two failed items are unacceptable unless the tester can find a good reason to justify these failures. With small sample sizes, any failure indicates that the control is ineffective. If the control fails, the tester must find out who is improperly performing the control, retrain the employee, and wait for a new population to build up. This means waiting several weeks or months before retesting the control.

Some companies have the philosophy that if testing produces two errors in a sample of 60, they will select another 60 items, and if no more errors occur, they will accept the control. The failure rates are based upon statistical reliability, so the company must be able to justify the failed items as statistically insignificant.

With SOX, sample size has been simplified, so project teams do not have to complete statistical calculations. If a control is performed daily, the population is 250, given 250 working days in a typical year. The project team then applies the required sample size for a population of 250. However, if a control is performed more than once daily, the population is greater than 250 (# of control performances each day x 250) and requires a much larger sample size.
**Chapter 4 – Test Plans**

<table>
<thead>
<tr>
<th>Functional Test Steps to be Performed</th>
<th>WP Ref</th>
<th>Sample Size</th>
<th>Document Request</th>
<th>Test Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obtain the sample of new vendors and date of setup. Perform a lookup to determine the number of the invoice processed on the setup date and obtain the hardcopy of the invoice. Verify the invoice has been approved by an individual with approval authority.</td>
<td>WP1</td>
<td>30</td>
<td>Report in Excel format from AP System of all vendors added in the current year and the date that the vendor was created.</td>
<td>&lt;Enter&gt;</td>
</tr>
<tr>
<td>Obtain the sample of checks and verify the supporting detail packet supports or ties to the check amount. Verify the GL coding sheet is attached and that the check signers have signed the packet as evidence of their review. (Signature may only be on check). Verify the individual signing the packet/check is authorized per the authorization lists (CEO, CFO, CAO, CLO Controller, Cashier, SVP/Operations, or Human Resources Officer).</td>
<td>WP2</td>
<td>30</td>
<td>Report in Excel format from AP System of all checks processed in the current year that also lists the payee, the amount and the check date.</td>
<td>&lt;Enter&gt;</td>
</tr>
<tr>
<td>Request that the Accounts Payable staff attempt to post an unbalanced batch from AP System to GL System. Verify that GL System will not allow the batch to post and obtain a screen print of the message.</td>
<td>WP3</td>
<td>1</td>
<td>None - System Test</td>
<td>&lt;Enter&gt;</td>
</tr>
<tr>
<td>Obtain the sample of batches / check registers from AP System and verify that Accounts Payable and another individual have initialed the corresponding Transaction Report as evidence that the upload to GL System was complete.</td>
<td>WP4</td>
<td>12</td>
<td>Report in Excel format from AP System of all Check Registers and the date that they were run / posted. Or a report from GL System of all batches posted and the date.</td>
<td>&lt;Enter&gt;</td>
</tr>
</tbody>
</table>

**A Sample Test Plan: Testing Summary**

The second tab in the test plan workbook is the testing summary. It aggregates the findings from all of the tabs that cover the individual controls (a small section of the testing summary is pictured above – test results are located in another column – See Appendix D for the complete testing summary document). The project team needs a quick summary of the test findings; that way it is not necessary to look through all the tabs to find out which tests passed and which failed. The easiest way to collect this information is to build cell-references into the summary sheet that link to the column listing whether or not the test passed for each of the individual control tabs.
A Sample Test Plan: Testing Summary Continued

The chart above is another detail taken from the testing summary tab of the test plan workbook. It shows the Test Result column (which uses the cell references described on the previous page) and columns labeled “Functional Test Steps to be Performed” and “Document Request.” These columns describe the testing procedures and required documents for each test. These columns also include cell references so that this information only has to be written once, on the testing summary tab; the cell references copy this information to the actual work paper tab for each given control. This also allows the project team to update the test plan quickly; any changes to testing procedures only need to be made on the summary tab, and not on each subsequent work paper tab. The column labeled “WP Ref” shows another nice feature: hyperlinks to the work paper tab so that the tester can quickly jump to the tab containing the detailed information about any particular test.
### A Sample Test Plan: The Test Work Paper

The chart above is a detail from a test work paper tab (see Appendix D for the complete work paper). It shows the test procedure (copied from the testing summary using the cell-reference feature of Excel®) and the columns listing attributes that the tester must check for each test item. For this particular control (EXP-02 from the Expenditure Cycle example), the tester needs to verify four different pieces of information (shown in columns 5-8; columns 1-4 identify each item in the sample).

<table>
<thead>
<tr>
<th>Ref #</th>
<th>Check #</th>
<th>Payee</th>
<th>$ Amount of Check</th>
<th>Date</th>
<th>Invoice or Support</th>
<th>GL Coding</th>
<th>Check Signer has Approved Packet</th>
<th>Check Signer is Authorized/ Appropriate</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Chapter 4 – Test Plans

New Testing ‘Season’

Strategy Alternative #1

<table>
<thead>
<tr>
<th>Q1</th>
<th>Q2</th>
<th>Q3</th>
<th>Q4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update documentation</td>
<td>Test</td>
<td>Re-test failures</td>
<td>Confirmation?</td>
</tr>
<tr>
<td>Confirmation</td>
<td>Confirmation</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

This first alternative is in relation to new SOX project or projects that have only been in place for a few years. Sampling should begin on January 1st and continue until the date of testing. The best time to begin the testing phase would be in the third quarter (July, August, and September). An exception to this would be an instance where a new control were put in place. If the new control were to go into effect on September 1st, then testing should be done from that point forward. Confirmations should be sent to process owners in the first and second quarters and fourth quarters for Section 302 compliance.

Strategy Alternative #2

<table>
<thead>
<tr>
<th>Q1</th>
<th>Q2</th>
<th>Q3</th>
<th>Q4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update documentation</td>
<td>Test</td>
<td>Re-test failures</td>
<td>Re-test failures &amp; high-risk</td>
</tr>
<tr>
<td>Confirmation</td>
<td>Confirmation</td>
<td>Confirmation</td>
<td>Confirmation</td>
</tr>
</tbody>
</table>

This second alternative is specifically for mature SOX projects. Sampling is done on a rolling basis so it should continue from the last date of previous testing to the first date of current testing. Testing is best done in the second quarter (April, May, and June). Confirmations should be sent to process owners in the first and third quarters for Section 302 compliance and in the fourth quarter for Section 404 compliance.
Chapter 4: Writing and Implementing Test Plans

Part 6: A Risk Based Approach to Testing III – Using A Random Number Generator
Excel® – Random Number Generator

The AbleBits® Random Number Generator Screenshot

The AbleBits® Random Number Generator

A random number generator is an essential tool for obtaining a sample that is statistically representative of the entire population. The random number generator pictured above can be downloaded free from the AbleBits® website and works as an Excel® plug-in.

With this simple tool, the tester need only highlight the cells for which a random number is required, and then select the AbleBits® plug-in. Then the tester can enter the range for the results, and the type of numbers desired (e.g. integers). The plug-in automatically fills in the cells with randomly generated numbers. While Excel® does have its own random number generator, it can be more confusing to use.
Randomly Selecting Test Items

Sample Output Using a Random Number Generator

The chart above shows the generation of random numbers for selecting a sample from a given population. The population is listed in the five columns at the left of the spreadsheet. The two columns in the upper right corner of the spreadsheet show that the tester needed 15 random numbers (shown in the first column at the right of the sheet) generated from the overall population of 30. The random number generator picked, at random, 15 of the members of the population (shown in the second column at the right of the sheet). Now, the tester simply has to find the selected items in the numbered population list.

The chart above also shows which members of the population were selected in the second column at the left. The tester can use Excel's® V-lookup function to easily indicate selected population items. V-lookup simply tells Excel® to look in the columns to the left of the sheet for the random numbers that were generated on the right of the sheet. If found, V-lookup places an "x" in the “selection” column, and if not, it records "N/A."
Chapter 4:
Writing and Implementing Test Plans

Part 7: A Risk Based Approach to Testing III – Test Exceptions
Test Exceptions

Test Exceptions

- Define exceptions (gaps) as any difference between what the control is designed to do and what the test results show.
- Examples of test exceptions:
  - Required signature is not present.
  - Review control is not performed.
  - Critical duties are not properly segregated.
  - Controls are not effective (will not prevent the risk).
  - System controls are not enabled.

Test Exceptions

If test items fail, the process owner needs to follow up with the employees completing the transactions to ensure that the control is applied properly. Given that 30% of a company's controls are likely to fail during the first year of the SOX compliance process, following up on test exceptions can be a huge job. Describing the risk and delegating the task of planning a remedy for the given deficiency to the process owner is the most effective way of solving control problems. Sometimes a company's personnel department will assign one employee to handle the follow-up work concerning control failures, but this is an overwhelming task for one person. The process owner already knows how the process works, and is thus ideally placed to help devise a solution.

Test Failure Form

Test Failure Form

4 Sections:
1. Tester’s Reason for Failing
2. Manager’s Evaluation
3. Process Owner’s Remediation
4. Evaluation Team Signs Off

The Deficiency Form

The chart above outlines the structure of a deficiency evaluation form (see Appendix E for a sample form). The form should have four sections. First, the tester's explanation of the failure; here the tester should explain the exceptions that he found. The tester should include some evidence to provide context for the failed test; for example, the failure was an isolated incident, or it only occurred in one location. This type of evidence is useful for the next section.

The second section is a manager's evaluation of the failed test. Because the tester might not have as much experience with SOX, it is important to have a manager evaluate each failed test. A manager's
evaluation is critical, because the company may have to undertake important changes to remedy the problem, and a tester should not shoulder the burden of initiating this kind of structural work. As part of the evaluation, the manager will recommend possible changes that the company could make.

After the manager evaluates the failure and makes a recommendation, the whole form is given to the process owner. The process owner either implements the changes recommended by the manager, or comes up with another way to solve the deficiency. Once the process owner has approved a remedy for the problem, he sends the form back to the project team. The project team then modifies the documentation if any controls have been changed, removed, or added.

Finally, a high-level employee at the company, usually someone on the disclosure committee, signs the form, accepting the failed test and approving the remedy.

It is crucial to have all four of these steps on one form because the external auditor will need to know which tests failed, and more importantly, the ways in which the company will correct the problems that led to the test failure. It is a good practice to put all of the test failure forms in a separate binder and to number them sequentially. This ensures that the external auditor can quickly find the important information about each failure and cross-reference it with the test plan and documentation.
Evaluating Deficiencies

- Look for compensating controls
- Isolate the amount

Evaluating Deficiencies

The chart above is included in the COSO *Small Business Guidance*; it can also be downloaded from website of the Institute of Internal Auditors (IIA). The chart was published December 20, 2004. The flowchart is designed to help the project team evaluate deficiencies; the top half shows how to check for a significant deficiency, while the bottom half shows ways to check for a material weakness. In essence, the chart proposes questions to help the auditor understand whether or not other controls would help the situation or if the dollar amount would remain below the threshold for a material weakness. For instance, perhaps, as in one of the earlier examples in the book, a management discussion and analysis (MD&A) would prevent a significant deficiency from becoming a material weakness. In meeting with the project manager, the company will want to avoid having material weaknesses, and will likely spend a great deal of time with this framework for thinking about controls that would limit the dollar amount of any given deficiency (AS #5 changed the definition of a significant deficiency to "reasonably possible" likelihood and an amount that "merits attention." The chart above was issued before this new guidance was adopted).
Chapter 5:  
Documenting & Testing IT General Controls

Part 1: IT Evaluation Frameworks
Frameworks for Documenting and Testing IT Controls

The auditor must choose from among the different frameworks available for the documentation and testing of the IT infrastructure. Pictured above is the cover of the framework published by the Information Technology Governance Institute (ITGI). The ITGI is a subset of CobiT, the IT equivalent of COSO.
**CobiT vs. SOX**

The ITGI developed its framework through a comparison of CobiT and PCAOB controls. By comparing the two, the ITGI produced the subset of CobiT controls described on the previous page. The chart above shows the comparison process.

### ITGI: Comparing CobiT and PCAOB Controls

The ITGI developed its framework through a comparison of CobiT and PCAOB controls. By comparing the two, the ITGI produced the subset of CobiT controls described on the previous page. The chart above shows the comparison process.

<table>
<thead>
<tr>
<th>IT Control Objectives for Sarbanes-Oxley</th>
<th>CobiT</th>
<th>PCAOB IT General Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Acquire and maintain application software.</td>
<td>A12</td>
<td>Program Development</td>
</tr>
<tr>
<td>2. Acquire and maintain technology infrastructure.</td>
<td>A33</td>
<td>Program Change</td>
</tr>
<tr>
<td>3. Enable operations.</td>
<td>A34</td>
<td>Computer Operations</td>
</tr>
<tr>
<td>4. Install and accredit solutions and changes.</td>
<td>A47</td>
<td>Access to Programs and Data</td>
</tr>
<tr>
<td>5. Manage changes.</td>
<td>A46</td>
<td></td>
</tr>
<tr>
<td>6. Define and manage service levels.</td>
<td>DS1</td>
<td></td>
</tr>
<tr>
<td>7. Manage third-party services.</td>
<td>DS2</td>
<td></td>
</tr>
<tr>
<td>8. Ensure systems security.</td>
<td>DS5</td>
<td></td>
</tr>
<tr>
<td>9. Manage the configuration.</td>
<td>DS9</td>
<td></td>
</tr>
<tr>
<td>10. Manage problems and incidents.</td>
<td>DS8, DS10</td>
<td></td>
</tr>
<tr>
<td>11. Manage data.</td>
<td>DS11</td>
<td></td>
</tr>
<tr>
<td>12. Manage the physical environment and operations.</td>
<td>DS12, DS13</td>
<td></td>
</tr>
</tbody>
</table>
Example of IT Control Objective

![Figure 15—Manage Changes](image)

<table>
<thead>
<tr>
<th>Illustrative Controls</th>
<th>Illustrative Tests of Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requests for program changes, system changes and maintenance (including changes to system software) are standardized, documented and subject to formal change management procedures</td>
<td>Determine that a documented change management process exists and is maintained to reflect the current process. Consider if change management procedures exist for all changes to the production environment, including program changes, system maintenance and infrastructure changes. Evaluate the process used to control and monitor change requests.</td>
</tr>
</tbody>
</table>

Rationale—Managing changes addresses how an organization modifies system functionality to help the business meet its financial reporting objectives. Deficiencies in this area could significantly impact financial reporting. For instance, changes to the programs that allocate financial data to accounts require appropriate approvals and testing prior to the change to ensure classification and reporting integrity.

Sample ITGI Control Objective

Like the COSO Small Business Guidance, the ITGI framework includes samples of controls such as the one shown above. The ITGI summarized the objective and the rationale for that objective. The ITGI also listed potential controls to help achieve the given objective. One nice feature included in the ITGI samples is a list of possible tests that the auditor can conduct for a particular control.
CobiT vs. Control Objectives vs. COSO

The three frameworks above are all important standards for evaluating the IT infrastructure. Large companies should consider the ITGI guidance while smaller business should use the COSO Small Business IT framework. CobiT’s original framework contained 34 condensed the list down to 12 objectives that are applicable under SOX. While the COSO objectives. By eliminating those that did not influence financial reporting, the ITGI framework is organized differently, it is even smaller than the ITGI framework and is useful for small companies.

<table>
<thead>
<tr>
<th>CobiT</th>
<th>IT Control Objectives for SOX</th>
<th>COSO (Small Business)</th>
</tr>
</thead>
<tbody>
<tr>
<td>34 Objectives</td>
<td>12 Objectives</td>
<td>10 Objectives</td>
</tr>
</tbody>
</table>
The COSO Small Business IT Framework

The chart above is a sample from the COSO Small Business Guidance volume on IT infrastructure (vol. 3).
Chapter 5: Documenting & Testing IT General Controls

Part 2: Testing IT General Controls
Typical IT General Controls Testing

- System Access & Account Maintenance
- Authentication
- IT Security
- Remote Access
- Wireless Networking
- Physical Security
- System Planning
- System Development
- Change Management
- Problem Management
- Backup & Restore
- IT Operations & Risk Assessment

Testing IT General Controls

The list above shows the possible areas of the IT infrastructure that the auditor must test. However, the three areas shown in large boldface type are most important to SOX. In terms of System Access and Account Maintenance, if an employee leaves the company, the company must remove their access privileges from the system. Since employees understand the way the IT infrastructure works, the chance of an ex-employee hacking into company IT systems and changing GL or payroll information is much greater than the possibility of an unaffiliated hacker altering the company accounts databases.

Changes in management are also important. New IT systems must be independently verified when they are installed. If for example, a company changes the way a particular program calculates depreciation, the company must have some assurance that the new calculations are correct.

Thirdly, the company must have secure and properly functioning backup and restoration modules. With reliable backup systems, the company can remedy problems with other systems by returning to the backup files.

In short, if the company has good controls on the three areas discussed above, the other areas of IT infrastructure will fall into line, and the company runs a much lower risk of a serious impact on financial reporting.
New PCAOB Standard – IT Benchmarking

- The extent to which the application control can be matched
- The extent to which the application is stable (i.e., there are a few changes from period to period); and
- The availability and reliability of a report of the compilation dates of the programs placed in production. (This information may be used as evidence that controls within the program have not changed.)

IT Benchmarking

IT benchmarking, as mentioned earlier in the book, is the reliance upon change controls instead of repeatedly testing applications. This is to say that if the company verifies that a given IT system functions properly when it is implemented or updated, it is not necessary to test that system every year as part of the SOX project.
IT Sample Testing

Check for:
- Approvals and oversight
- Appropriateness
- Documents (evidence) retained
- Built-In system controls exist & are working
- Alerts are working and logs are reviewed (monitoring)

IT Testing Issues

When conducting IT infrastructure testing, the project team should consider the attributes listed above. Approvals and oversight are self-explanatory. Documents retained simply means that the company must keep records. Built-in system controls should exist and function properly. The last attribute is one of the most critical. The company must have an employee monitor system alerts and logs. If for example, IT system reports indicate that hackers have made intrusion attempts, someone should follow up on these reports and “plug the hole.”
Chapter 5:  
Documenting & Testing IT General Controls  

Part 3: Segregation of Duties Testing
IT Testing and Segregation of Duties

The three primary ways to evaluate segregation of duties issues are listed above. Most companies rely upon the process of developing a risk and control matrix as a means of thinking through segregation of duties issues. The second method is to prepare a separate segregation of duties matrix for each cycle. The third technique requires combining data from the IT systems with a manual assessment of segregation of duties to incorporate as much information as possible into the evaluation.
1. Risk & Controls Matrix

<table>
<thead>
<tr>
<th>Process Code</th>
<th>Process Risk Code</th>
<th>Objective Code</th>
<th>Objective Description</th>
<th>Risk Code</th>
<th>Risk Description</th>
<th>Control Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXP-01 Vendor setup</td>
<td>Low</td>
<td>Env</td>
<td>Only valid vendors are added to or maintained in the vendor master file</td>
<td>Risk</td>
<td>Invalid vendors added to file</td>
<td>Fraudulent or invalid changes are made to vendors in the vendor master file. Accounts Payable verifies that all invoices from new vendors are approved for validity prior to adding the vendor to the vendor master file.</td>
</tr>
<tr>
<td>Low</td>
<td>Env</td>
<td>Only valid vendors are added to or maintained in the vendor master file</td>
<td>Risk</td>
<td>Invalid vendors added to file</td>
<td>Fraudulent or invalid changes are made to vendors in the vendor master file.</td>
<td></td>
</tr>
<tr>
<td>Low</td>
<td>Env</td>
<td>Only Vendor File remains valid</td>
<td>Risk</td>
<td>Invalid Vendors not detected</td>
<td>Inappropriate or inaccurate changes and/or additions to the vendor master file are not detected in a timely manner.</td>
<td></td>
</tr>
</tbody>
</table>

**Issues:**
- Hard to think of all possible conflicts
- Over reliance on process owner representations
- Uncoordinated analysis of system access

The Risk & Control Matrix and Segregation of Duties

Using the risk and control matrix is probably the least comprehensive way to address the segregation of duties. The project team is sure to miss important segregation of duties issues using the risk and control matrix as their only evaluation tool. This method also relies too heavily on the process owner’s self-report. The result is a very uncoordinated analysis. In the past, many companies avoided conducting separate segregation of duties testing by stating that it was covered in the risk and control matrix. However, these companies almost certainly overlooked potential problems.
2. SOD Matrix

The Segregation of Duties Matrix

The second method of evaluating segregation of duties issues involves developing a separate matrix to analyze the relationships between employees and functions within a process. This is preferable to using the risk and control matrix alone. The principle is that certain employees can authorize transactions, others can record transactions or have custody of assets, and still others can perform controls. The company wants to avoid situations in which someone authorizes and records transactions (or any other combination of different functions, such as authorizing and having custody of assets or recording and having custody of assets). Ideally, each employee should only perform functions in one area (the color coded segments at the top of the matrix). When a given employee's duties fall into two categories, as in the case of the functions circled on the chart above, the auditor should explain whether or not the given situation poses a problem.

This is a good method of evaluating segregation of duties, but it still cannot capture all of the possibilities. Like the risk and control matrix, it too relies upon employee self-reports. The employee may not remember all of the privileges that the IT system gives him. As a result, the auditor must check the IT system as well to catch any access privileges that the employee may have omitted (often employees can forget about duties that require system access on a very infrequent basis).

SOD Matrix Issues:
- Over reliance on process owner representations
- Uncoordinated analysis of system access
3. Export System Access data and combine with Manual Activities

Segregation of Duties: A Hybrid Evaluation Technique

The most sophisticated and complete method of documenting and testing segregation of duties issues involves combining data from the IT system with a list of manual activities for a given cycle. An example of a manual activity is reconciling bank accounts. The IT system cannot identify who completes this task. However, the project team can create a database to combine IT privileges with manual responsibilities to generate a report identifying conflicts. Most external auditors do not yet ask for this level of detail, but they are quickly learning to make this a standard practice.
Chapter 6: Documenting & Testing IT General Controls

Part 1: Spreadsheet Controls
Spreadsheet Controls:

A recent number of restatements resulted from spreadsheet errors. Spreadsheets are the most common tool used in finance and accounting organizations. Generally, individuals believe spreadsheets are prepared correctly; however, studies over the prior 10 plus years (see http://panko.shidler.hawaii.edu) find the majority (greater than 85%) of spreadsheets with more than 150 lines contain significant (not minor) formatting errors.

There are five major categories of spreadsheet errors: input errors, output errors, no audit trail; no version control and limited security. In addition to the concerns listed above, spreadsheets are frequently the source of recording entries in the general ledger. Input errors arise from simple typographical errors, information cut and pasted into the wrong section of the spreadsheet and the input not properly updated due to settings such as manual recalculation selected and the unnoticed. Output errors are primarily due to incorrect formula errors. Most organizations do not maintain an audit trail of changes made to spreadsheets. This results in unauthorized changes, especially without the knowledge of the spreadsheet reviewer. The lack of version control has resulted in an incorrect spreadsheet being used (outdated, incomplete or containing erroneous information). Lastly, the lack of security enables most of the above weaknesses.

Good spreadsheet controls are an important component of a strong controls as they typically result in entries to the general ledger.

Controls to Mitigate Spreadsheet Risks

- Change Control
- Version Control
- Access Control
- Input Control
- Security Control
- Documentation
- Development Lifecycle
- Back-ups
- Archiving
- Logic Inspection
- Segregation of Duties
- Overall Analytics

The table above lists twelve controls that can mitigate the risks of material misstatements in the financials due to spreadsheet errors.

Implementing strong spreadsheet control begins with an inventory of critical spreadsheets. Spreadsheet control also includes ensuring there is a formal process for testing and approving changes prior to re-use of the spreadsheet. Just as there would be a formal process for changes made to the company ERP system, managing critical spreadsheets in the same manner will mitigate spreadsheet control risk.

Many individuals may have access to critical shared network drives at the company. To maintain control over critical company data the company should implement version control and access control. Version control ensures that the current spreadsheet is used, which may be important when a spreadsheet is revised and updated on a monthly basis. Establishing access control to limit unauthorized use of critical spreadsheets is imperative. Implementing restricted access through the network, workstations or using passwords to protect the individual workbook or spreadsheet are valid ways to strengthen spreadsheet controls.
Next, the company should be concerned about input controls. Uses of desktop tools are common methods to extract data from the company business system and input it into a spreadsheet that generates an accounting entry. Ensuring the cell area is properly designed and adequate to accept input (cut and paste from other applications) is as critical as typographical errors that may occur (such as transposing numbers). Performing a reconciliation between the accounting system and data used in the spreadsheet provides a strong control over input errors.

Implementing security control features that are standard in spreadsheet applications can prevent inadvertent errors such as overwriting a critical formula. Designing spreadsheets with areas that are locked or protected strengthen spreadsheet controls. In addition, an independent reviewer should check the logic and critical formulas in the spreadsheet.

Documentation provides critical information about the spreadsheet, such as the purpose and instructions for using the spreadsheet. The documentation created in a separate tab in the spreadsheet, provides the user needed information.

A development lifecycle should include specific processes for identifying spreadsheet requirements, specifications, design, building, testing and maintenance activities.

IT general controls typically address the back-up of critical application files. It is important to review that back-ups are regularly scheduled and retrievable for critical spreadsheets as well. The IT infrastructure department should ensure backup of spreadsheets- on local PCs and shared files on the network.

Implementing an archiving strategy to ensure the correct version of a spreadsheet is used strengthens controls. Prior versions of spreadsheets should be segregated in a separate directory and saved as “read-only.”

Segregation of duties over spreadsheets is accomplished by clearly defining roles and ownership.

Embedding analytics and reasonableness checks into spreadsheets can mitigate the risk of significant errors. Reasonableness checks are alternative calculations of the spreadsheet result using summary data. The reasonableness check figure is then compared to the actual figure calculated in the spreadsheet. For instance a vacation accrual calculated by employee could be checked for reasonableness by calculating a vacation accrual using total number of employees and an average unpaid vacation.

Combining the controls outlined above will ensure the company has generated correct data from spreadsheets.
The table above is a listing of commercially available tools to assist with spreadsheet controls. This list should provide the reader with a place to begin an evaluation of commercially available tools.
Chapter 6: Excel, Access, and Web-Based Applications

Part 2: Choosing Useful Software Applications
Varieties of Software Tools

The above chart shows some of the important characteristics of three types of software tools available to the SOX professional. Each tool has its own strengths and weaknesses, highlighted above. Another available tool is SarbOxPro®, developed by Cost Advisors, Inc. A free download is available from the SarbOxPro.com website.
Using Excel®, Word® and Visio®

Using separate applications, such as Excel®, Word®, and Visio®, is certainly a viable means of conducting a project. The drawback is that the project team must coordinate and organize the hundreds of files they will create during a SOX project. Furthermore, each time a given control is used requires a repeated row in Excel®. Whereas in a database, the control is placed into a data table just once (this is referred as “data normalization” by programmers).
Saving Work Documents in a Database

Using a database to store the many work documents that a project generates is a convenient organization method. This allows the project team members to quickly locate any of the files generated through the various applications used (e.g. Word®, Excel®, Visio®).
Chapter 7:
Summary of Sarbanes-Oxley 404 Best Practices
Summary of Best Practice Ideas

- Implement a risk-based approach
- Multiple locations, processes and controls evaluated based on risk
- External auditor reliance on internal testing
- Substitute company-level controls for process-level controls
- Exclude unnecessary processes
- Document with swim-lane flowcharts
- Ignore non-key controls
- For IT:
  - Focus testing on: System Access, Backups and Change Control
  - Use Benchmarking

Sarbanes-Oxley Best Practices Summary

The list above shows the best practices covered in this book. Most important is the implementation of a risk-based approach. Following this concept, the project team should evaluate each company location based upon its level of risk and should not use a coverage-based model. Another important practice is to work with the external auditors so that they can rely upon the quality of work produced internally. Using company level controls, where they are sensitive enough, allows savings of time and money on the project. The project team should also concentrate on eliminating from the evaluation any processes that do not influence financial reporting. Swim-lane flowcharts offer many benefits over creating a narrative to document a given business process. Under the new Auditing Standard#5, the project team can omit non-key controls from the project as well. Lastly, when testing the IT infrastructure, the team should emphasize System Access, Change Control, and Backup systems. These are key areas that can obviate the need for testing other parts of the infrastructure.

Applying the best practices described in this book will save the evaluation team time and money, while producing a highly effective, comprehensive SOX compliance project.
**Summary**

**Proposed Next Steps**

1. Ensure buy-in from management
2. Form Steering Committee
3. Hire Project Manager
4. Decide Materiality, Scope, & Schedule
   - Identify specific processes
   - Identify process owners
5. Hire Documentation & Testing Resource

**Critical Steps in Sarbanes-Oxley Planning**

Following the steps outlined above can lay the foundation for a successful SOX project. Support from upper management gives the project team a legitimate status as they conduct their work. The steering committee can provide guidance to the project team along the way. The project manager is an essential member of the team who coordinates the project, publicizes it within the company, and acts as the liaison to the steering committee as well as to the external auditors. Deciding scope, schedule and materiality places important boundaries on the project, keeping it manageable and within budget. The last step in the setup process is to hire well-qualified documentation and testing staff to complete the project.

**Key Take-Aways**

- Our goal is to prepare for management’s attestation
- Best practices are now known
- Project organization and an experienced team is the key to efficiency
Summary

Keys to Sarbanes-Oxley Success

Because the goal of a SOX project is to prepare documentation for management attestation, the best practices explained in this book give the project team the most effective tools for meeting a client's needs. A well-planned project executed by an experienced team is the key to efficiently and comprehensively complying with the Sarbanes-Oxley Act.
Appendix A:
List of Processes
<table>
<thead>
<tr>
<th>Process Code</th>
<th>Process Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>ENT-01 Integrity</td>
<td>Management's approach to Integrity and Ethics</td>
</tr>
<tr>
<td>ENT-02 Competency</td>
<td>Management's dedication to Competency at all levels of the enterprise</td>
</tr>
<tr>
<td>ENT-03 Oversight</td>
<td>Role of the Board of Directors or Audit Committee in Overseeing Entity Level Controls</td>
</tr>
<tr>
<td>ENT-04 Ideology</td>
<td>The overall Ideology and operating style of management, effecting the entity in many intangible ways</td>
</tr>
<tr>
<td>ENT-05 Structure</td>
<td>The appropriateness of the design of the organizational Structure</td>
</tr>
<tr>
<td>ENT-06 Authority</td>
<td>The allocation of Authority and its relation to control and accountability</td>
</tr>
<tr>
<td>ENT-07 Human Resources</td>
<td>Role of Human Resource activities and policies in promoting the organizations goals</td>
</tr>
<tr>
<td>ENT-08 Risk Assessment</td>
<td>Entity Risk Assessment</td>
</tr>
<tr>
<td>ENT-09 Control Activities</td>
<td>Entity Control Activities</td>
</tr>
<tr>
<td>ENT-10 Entity Monitoring</td>
<td>Entity Monitoring</td>
</tr>
<tr>
<td>ENT-11 Info &amp; Communication</td>
<td>Entity Information &amp; Communication</td>
</tr>
<tr>
<td>EXP-01 Vendor setup</td>
<td>Vendor setup</td>
</tr>
<tr>
<td>EXP-02 Purchase Req</td>
<td>Creating Purchase Requisitions</td>
</tr>
<tr>
<td>EXP-03 Purchasing</td>
<td>Purchasing</td>
</tr>
<tr>
<td>EXP-04 Receiving</td>
<td>Receiving Goods</td>
</tr>
<tr>
<td>EXP-05 Returns</td>
<td>Returns to Vendors</td>
</tr>
<tr>
<td>EXP-06 Invoice Processing</td>
<td>Invoice Processing</td>
</tr>
<tr>
<td>Code</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>EXP-07</td>
<td>Payment Processing</td>
</tr>
<tr>
<td>EXP-08</td>
<td>AP Accrual (Incl Received not Invoiced)</td>
</tr>
<tr>
<td>FIN-01</td>
<td>Chart of Accounts Maintenance</td>
</tr>
<tr>
<td>FIN-02</td>
<td>Capturing/Recording Estimates &amp; Accruals</td>
</tr>
<tr>
<td>FIN-11</td>
<td>Prep Financial Disclosures</td>
</tr>
<tr>
<td>FIN-12</td>
<td>Close GL</td>
</tr>
<tr>
<td>FIN-13</td>
<td>Post-Close Adjusting Entries</td>
</tr>
<tr>
<td>FIN-14</td>
<td>Prep Financial Statements</td>
</tr>
<tr>
<td>FIN-15</td>
<td>Non-Operating Income</td>
</tr>
<tr>
<td>FIN-16</td>
<td>Non-Operating Expense</td>
</tr>
<tr>
<td>FIX-01</td>
<td>Fixed Asset Balances</td>
</tr>
<tr>
<td>FIX-02</td>
<td>Asset Acquisition</td>
</tr>
<tr>
<td>FIX-03</td>
<td>Fixed Asset Delivery &amp; Installation</td>
</tr>
<tr>
<td>FIX-04</td>
<td>Fixed Asset Set-up</td>
</tr>
<tr>
<td>FIX-05</td>
<td>Assets Leased from Others</td>
</tr>
<tr>
<td>FIX-06</td>
<td>(Not Used)</td>
</tr>
<tr>
<td>FIX-07</td>
<td>Internally Developed Assets</td>
</tr>
<tr>
<td>FIX-10</td>
<td>Depreciation and Amortization</td>
</tr>
<tr>
<td>FIX-11</td>
<td>Asset Impairment (tangible assets)</td>
</tr>
<tr>
<td>FIX-12</td>
<td>Asset Disposal - Procedures &amp; Accounting</td>
</tr>
<tr>
<td>PAY-01</td>
<td>Hiring &amp; Termination - Authorization</td>
</tr>
<tr>
<td>PAY-04</td>
<td>Timecard Processing</td>
</tr>
<tr>
<td>Code</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>--------------------------------------</td>
</tr>
<tr>
<td>PAY-06</td>
<td>Calculating PR</td>
</tr>
<tr>
<td>PAY-09</td>
<td>Vac &amp; PR Accruals</td>
</tr>
<tr>
<td>INV-01</td>
<td>Inbound Cutoff</td>
</tr>
<tr>
<td>INV-03</td>
<td>Whse Mvmt &amp; Bal</td>
</tr>
<tr>
<td>INV-05</td>
<td>Invty Reserves</td>
</tr>
<tr>
<td>ITG-01</td>
<td>Financial Reporting &amp; Systems</td>
</tr>
<tr>
<td>ITG-02</td>
<td>Financial Reporting &amp; IT infrastructure</td>
</tr>
<tr>
<td>ITG-03</td>
<td>System Updates Procedures</td>
</tr>
<tr>
<td>ITG-04</td>
<td>System Testing</td>
</tr>
<tr>
<td>ITG-05</td>
<td>Modification Testing</td>
</tr>
<tr>
<td>ITG-06</td>
<td>System Maintenance</td>
</tr>
<tr>
<td>ITG-07</td>
<td>Outsourced IT Functions</td>
</tr>
<tr>
<td>ITG-08</td>
<td>Financial Reporting System Security</td>
</tr>
<tr>
<td>ITG-09</td>
<td>System Protection</td>
</tr>
<tr>
<td>ITG-10</td>
<td>Failure Response</td>
</tr>
<tr>
<td>ITG-11</td>
<td>Data Integrity</td>
</tr>
<tr>
<td>ITG-12</td>
<td>System Performance</td>
</tr>
<tr>
<td>MFG-01</td>
<td>BOM</td>
</tr>
<tr>
<td>Code</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>MFG-02</td>
<td>MFG-02 Std Cost - Mat'l Standard Costs - Material</td>
</tr>
<tr>
<td>MFG-03</td>
<td>MFG-03 Std Cost - L&amp;OH Standard Costs - Labor &amp; Overhead</td>
</tr>
<tr>
<td>MFG-05</td>
<td>MFG-05 Prod'n Plan Production Planning</td>
</tr>
<tr>
<td>MFG-06</td>
<td>MFG-06 Building Inventory Building Inventory, Tracking WIP</td>
</tr>
<tr>
<td>MFG-08</td>
<td>MFG-08 Variances Manufacturing Variances</td>
</tr>
<tr>
<td>MFG-09</td>
<td>MFG-09 Scrap Manufacturing Scrap &amp; Rejects</td>
</tr>
<tr>
<td>REV-01</td>
<td>REV-01 Pricing Price Setting - Normal</td>
</tr>
<tr>
<td>REV-03</td>
<td>REV-03 Customer Orders Receiving &amp; Processing Customer Orders</td>
</tr>
<tr>
<td>REV-05</td>
<td>REV-05 Sales Tax Sales Tax - Charging &amp; Accounting</td>
</tr>
<tr>
<td>REV-07</td>
<td>REV-07 Outbound Cutoff Outbound Shipments Cutoff</td>
</tr>
<tr>
<td>REV-08</td>
<td>REV-08 Invoicing Customer Invoicing</td>
</tr>
<tr>
<td>REV-09</td>
<td>REV-09 Leasing Revenue Product Leasing Revenue</td>
</tr>
<tr>
<td>REV-12</td>
<td>REV-12 Bad Debts Bad Debt Allowance (Reserve)</td>
</tr>
<tr>
<td>REV-13</td>
<td>REV-13 Write Offs Bad Debt Write Offs</td>
</tr>
<tr>
<td>REV-14</td>
<td>REV-14 Customer Returns Customer Returns</td>
</tr>
<tr>
<td>REV-24</td>
<td>REV-24 Sales Comm Salesperson Commission - Plan, Accrual, Payment</td>
</tr>
<tr>
<td>TAX-01</td>
<td>TAX-01 Prov &amp; Def Tax Tax Provision &amp; Deferred Tax Accounting</td>
</tr>
<tr>
<td>TAX-02</td>
<td>TAX-02 Interco Prices Intercompany Pricing</td>
</tr>
<tr>
<td>TRE-01</td>
<td>TRE-01 Depositing Cash Depositing Cash</td>
</tr>
<tr>
<td>TRE-04</td>
<td>TRE-04 Investments-recording Sales &amp; Purch of investments-recording</td>
</tr>
<tr>
<td>TRE-05</td>
<td>TRE-05 Derivatives Derivatives</td>
</tr>
<tr>
<td>TRE-20</td>
<td>TRE-20 Debt Issuing &amp; Repaying Debt</td>
</tr>
<tr>
<td>TRE-21 Stock</td>
<td>Stock Issuance &amp; Repurchase</td>
</tr>
</tbody>
</table>
Appendix B:
Sample Flowchart for Expenditure Cycle
(File name: Visio-EXP Cycle Flow 03-22-07.pdf)
Appendix C:
Risk Evaluation Spreadsheet
Free downloads of this Spreadsheet and more are available at [www.SarboxPro.com](http://www.SarboxPro.com) (File name – Risked-Based Approach to Testing.xls)
Appendix D:
Sample Test Plan for Expenditure Cycle
The nature of tests can be classified into four categories: inquiry, observation, examination, and reperformance. The more significant the activity relative to risk (the "high impact and high probability" rankings from the risk assessment) the more important it is to ensure that the testing selected provides sufficient evidence of control effectiveness. The level of assurance is also affected by the category chosen. The categories listed above are in the order of lower assurance to higher assurance.

For example, asking about the existence of a control (inquiry) is less reliable than selecting evidence and examining for proof the control was performed. The highest degree of assurance comes from reperforming the control. Combining two or more of these tests also provides greater assurance than using only one test. As an example, consider the footing of a table of numbers or the financial statements. Re-footing the numbers is more reliable than verifying the "tick" marks used to indicate the footing was performed. However, the mere absence of any errors in the re-footing does not provide conclusive evidence that the footing control has historically been performed. The combination of both an error free reperformance and verifying the "tick" marks would provide better evidence of effectiveness (error free indicates performing as intended and the "tick" marks provided evidence that the control was performed).

Be skeptical of evidence that is documented solely by the initials of a performer, where the examination of the initials provides little evidence of the effectiveness of the control activity. Documentation of reconciliations, including follow-up and resolution of unusual items, may contain information that provides the true evidence of effectiveness.

The type of evidence may dictate what type of test is performed. Tangible evidence can usually be selected as a sample and examined. However, intangible or soft evidence may restrict the testing to inquiry or observation. "Restricted access" may be a control that can only be verified by inquiry or observation and does not lend itself to an examination of tangible evidence.

### Population & Sample Size Guidelines

**Define the population**
- Determine the appropriate population for the control being tested. Ensure the population is valid (for example: ties to GL or activity in an unusual category)
- Select the sample
- Sample sizes have been standardized based on the risk of the process / control and the frequency of the performance of the control
- Sample sizes listed below are minimum sample sizes and may be adjusted upwards to reflect the risk of the process / control

**NOTE:** In certain situations, the frequency of the performance of the control may not be an adequate indicator of the population size.

(Example - a control may be performed monthly but is performed monthly for each employee or invoice, etc. The population size is not 12 and therefore the sample size suggested for a monthly control is not appropriate.) In situations such as this, determine the population size and determine if the appropriate sample size based on the chart below.

**NOTE:** Population definition / determination and sample selection must be adequately documented for re-performance.

#### Minimum Sample Sizes by Risk:

<table>
<thead>
<tr>
<th>Control Frequency</th>
<th>Initial</th>
<th>Roll Forward</th>
<th>Initial</th>
<th>Roll Forward</th>
<th>Initial</th>
<th>Roll Forward</th>
<th>Low Risk</th>
<th>Med Risk</th>
<th>High Risk</th>
<th>Total Sample</th>
<th>Population Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Many X / Day</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>30</td>
<td>30 60</td>
<td>12 25</td>
<td></td>
<td></td>
<td>Up to 365</td>
<td>&gt; 365</td>
</tr>
<tr>
<td>Daily</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>12</td>
<td>12 25</td>
<td></td>
<td>4 4 4</td>
<td>12</td>
<td></td>
<td>52</td>
</tr>
<tr>
<td>Weekly</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2</td>
<td>2 2</td>
<td>2</td>
<td>1 1 1</td>
<td>1</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Monthly</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Quarterly</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Semiannually</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Annually</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Exceptions:**

Exceptions are instances discovered during the testing process where the control activity in place is either not designed or executed appropriately to mitigate the risk identified. When the control activity is not executed in a manner which is effective in mitigating the identified risk, the tester needs to determine if the situation warrants additional testing.

Finding several errors during the testing of the sample items would indicate a gap and require the development of a remediation plan related to the control activity.

Alternatively, one error may be encountered during the testing and the Testing Resource does not believe the error is representative of normal operations. Additional analysis and testing may provide statistical support for accepting the test findings as Effective (the errors encountered were not statistically significant).

<table>
<thead>
<tr>
<th>Control Frequency</th>
<th>Tolerance</th>
<th>Action</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Many X / Day</td>
<td>1 or more</td>
<td>The tester will need to perform additional analysis and testing to provide statistical support for accepting the test findings as Effective (errors were not statistically significant).</td>
<td></td>
</tr>
<tr>
<td>Daily</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Weekly</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monthly</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Quarterly</td>
<td>0</td>
<td>With small sample sizes, any exception leads to control failure.</td>
<td></td>
</tr>
<tr>
<td>Semi-Annually</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Annually</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Process Code</td>
<td>Risk Rating</td>
<td>Control Type</td>
<td>Control Code</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
<td>--------------</td>
<td>--------------</td>
</tr>
<tr>
<td>EXP-01 Vendor setup</td>
<td>Low</td>
<td>Manual</td>
<td>EXP-01</td>
</tr>
<tr>
<td>EXP-01 Vendor setup</td>
<td>Low</td>
<td>Manual</td>
<td>EXP-02</td>
</tr>
<tr>
<td>WP9</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WP8</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WP6</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WP5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WP3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WP2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WP1</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Workbook Tab 3: Work Paper 1  (File name: EXP Test Plan WP1 03-23-07.pdf)

TEST DETAIL:

<table>
<thead>
<tr>
<th>Test Cycle:</th>
<th>Expenditures</th>
<th>Test Name:</th>
<th>EXP-01 Vendor setup</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Reference #:</td>
<td>EXP-01</td>
<td>Control Owner:</td>
<td>Accounts Payable</td>
</tr>
</tbody>
</table>

CONTROL DESCRIPTION:
Accounts Payable verifies that all invoices from new vendors are approved for validity prior to adding the vendor to the vendor master file.

POPULATION:
All vendor additions and changes recorded during the test period.

SAMPLE:
Request Accounts Payable to run the Vendor Additions Report in AP System for the current year to date. Export list to an Excel spreadsheet and select a random sample of vendor additions.

TEST PROCEDURE:
Obtain the sample of new vendors and date of setup. Perform a lookup to determine the number of the invoice processed on the setup date and obtain the hardcopy of the invoice. Verify the invoice has been approved by an individual with approval authority.

TEST SELECTIONS:

<table>
<thead>
<tr>
<th>Ref #</th>
<th>Vendor Name</th>
<th>Date of Setup</th>
<th>Invoice #</th>
<th>Proper Approval Obtained</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>21</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>22</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>23</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>24</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>25</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>26</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>27</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>28</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>29</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>30</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

NOTES: WP Specific

CONCLUSION:
Deviations Identified | <Enter> | Additional Testing Required? | <Enter> | Control Activity Conclusion | <Enter>

Pass || Pass with Exception || Fail
If this symbol is used, enter detail in the Notes column.
TEST DETAIL:

Test Cycle: 
Process Ref & Title: EXP-01 Vendor setup
Control Reference #'s: EXP-02
Control Owner: Authorized Signers are CEO.

CONTROL DESCRIPTION:
Check signers verify the invoice is valid, and the check amount and GL coding are accurate prior to signing the check.

POPULATION:
All checks processed during the testing period.

SAMPLE:
30

TEST PROCEDURE:
Obtain the sample of checks and verify the supporting detail packet supports or ties to the check amount. Verify the GL coding sheet is attached and that the check signer has signed the packet as evidence of their review. (Signature may only be on check). Verify the individual signing the packet/check is authorized per the authorization lists (CEO, CFO, CAO, CLO Controller, Cashier, SVP/Operations, or Human Resources Officer).

TEST SELECTIONS:

<table>
<thead>
<tr>
<th>#</th>
<th>Check #</th>
<th>Payee</th>
<th>$ Amount of Check</th>
<th>Date</th>
<th>Invoice or Support Ties to Check Amount</th>
<th>GL Coding Attached</th>
<th>Check Signer has Approved Packet</th>
<th>Check Signer is Authorized / Appropriate</th>
<th>Notes: Line Item Specific</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

NOTES: WP Specific

CONCLUSION:

Deviations Identified: <Enter>
Additional Testing Required?: <Enter>
Control Activity Conclusion: <Enter>

Testing Performed By: <Enter>
Tester Name: <Enter>
Test Date: <Enter>
Key Contact: <Enter>

Pass •
Pass with Exception ●
Fail ●

If this symbol is used, enter detail in the Notes column.
Appendix E: Deficiency Evaluation Form
Inappropriate or inaccurate changes and/or additions to the vendor master file are not detected in a timely manner.

There are no controls in place for an individual independent of AP to periodically review the vendor master file for accuracy and ongoing pertinence. EXP-01

Was this a Test Failure?
What is the cause of the test failure?
Are there compensating controls? (list)

Test Failure Information:

Would there be an impact to the Financial Statement? ($$)

Financial Statement Impact:

Program Management Office Only:

Exception Classification:

Restest? If Yes:
Resume Regular Test Schedule
Additional testing ___ selections in Qtr___

Process Owner:

Please describe the action(s) taken to remediate the control deficiency.

Briefly describe how these actions address the risk.

Documentation changes required?

Flow Chart
Rate & Controls

SOX Program Management Office Review / Approval:

Date
Glossary:
Important Terms and Acronyms
Glossary of Important Terms and Acronyms

AICPA – American Institute of Certified Public Accountants – the AICPA is the national professional organization for certified public accountants.

A/P – Accounts Payable – Short-term debt, shown as a current liability on the balance sheet, which a company incurs for the products or services purchased.

A/R – Accounts Receivable – Monetary balance, shown as a current asset on the balance sheet, which a company receives for the products sold or services rendered.

AS – Auditing Standard – These documents are the primary publications of the PCAOB and determine the practices that must be followed by firms auditing firms.

Chart of Accounts – The chart of accounts is a listing of all the accounts in the general ledger with a reference number for each account.

CobiT – Control Objectives for Information and related Technology – Developed by ISACA (formerly known as the Information Systems Audit and Control Association), COBIT is an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks. More information about CobiT can be found on the ISACA website at http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=31519.

Company Level Controls – This is another term for entity level controls. This is similar to “tone-at-the-top” and control environment.

Cycle – A cycle is a collection of related processes. Some companies refer to cycles as processes; these companies refer to subprocesses where this book discusses processes within a cycle.

Entity Level Controls – These controls ensure that the corporate environment is free of corruption and holds itself to a set of values that promote ethical business practices.

FAS 5 – Financial Accounting Standard 5 – This statement establishes standards of financial accounting and reporting for loss contingencies. More information about FAS 5 including the full text of the statement can be found at http://www.fasb.org/st/.


GAAP – Generally Accepted Accounting Principles – Standards that governs accounting practices for public and private organizations. GAAP are overseen by the Financial Accounting Standards Board.

GL – General Ledger – A record that all the final transactions are posted in order to prepare the financial statements. General ledger accounts also reports the totals of the subsidiary accounts such as A/P accounts and A/R accounts.

Heat Sheet – A heat sheet is a chart that maps testing standards as a function of inherent process risk and risk of control failure, graphically representing the level of evidence that should be used to evaluate a control or set of controls.

ICFR – Internal Control over Financial Reporting – ICFR, pronounced “ick’ if er” by Sarbanes-Oxley pros, refers to the set of standard practices that a company must follow in documenting its financial situation. ICFR mandates that a company must keep its own records, that transactions roll up to financial statements that comply with GAAP, that management must authorize all receipts and expenditures, and that a company must protect its assets.

IT – Information Technology – This includes the computer infrastructure and software modules that help automate a company’s activities.

ITGI – Information Technology Governance Institute – ITGI is a research think tank that exists to be the leading reference on IT-enabled business systems governance for the global business community. More information about ITGI can be found at http://www.itgi.org/.
ITGC – Information Technology General Controls – ITGC is a broad foundation of the IT control structure to ensure reliability and integrity of financial reporting. The three most important ITGC areas in SOX are system access and account maintenance, change management, and backup and recovery.

Key Control – A key control is the control upon which a company is relying to prevent a specific risk. While not necessarily the only control for a given risk, the key control is the one that the company considers most important.

MD&A – Management’s Discussion and Analysis of Financial Condition and Results of Operations – A section of the annual report that designed to elicit disclosures that will allow investors to understand the current and expected future operating results and financial condition of a company, including the potential effects of known trends, commitments, events and uncertainties. According to the SEC, “MD&A is intended to give investors an opportunity to look at the company through the eyes of management by providing both a short and long-term analysis of the business of the company.”

MW – Material Weakness – A material weakness is a condition in which internal controls do not reduce to a relatively low level the risk that material errors or fraud may occur and not be detected in a timely period by employees in the normal course of their duties. Material weaknesses must be reported not only to the Board but also to the shareholders of a company.

PCAOB – Public Company Accounting Oversight Board – Created by the Sarbanes-Oxley Act of 2002, the PCAOB (pronounced “peek-a-boo” by those familiar with Sarbanes-Oxley work) is a private, non-profit organization that reviews the practices of firms auditing public companies to ensure that audit reports are informative, fair, and independent. More detailed information about the PCAOB can be found at http://www.pcaobus.org/.

Process – A financial process is a series of job activity that deal with transactions that will ultimately end up in the company's financial statements. Some companies refer to processes as subprocesses; these companies refer to entire cycles as processes.

SAS 70 – Statement of Auditing Standards # 70 – Developed by the AICPA, SAS 70 sets requirements for audits of service providers who contract out to public companies. Because public companies need to test controls that the service providers perform, SAS 70 allows these service providers to have one external audit conducted; they then make the results available to their clients for Sarbanes-Oxley compliance.

SAS 73 – Statement of Auditing Standards # 73 – SAS 73 provides guidance to the auditor who uses the work of a specialist.

SD – Significant Deficiency – A deficiency is an internal control shortcoming or opportunity to strengthen internal controls. A significant deficiency is a deficiency that meets the criterion of meriting attention by the company’s governing body or Board of Directors. Significant deficiencies must be reported to the company audit committee.

SEC – Securities & Exchange Commission – The SEC was created by the Securities Exchange Act of 1934 to help restore investor confidence after the stock market crash of 1929. To this end, the SEC monitors the financial reporting practices of public companies. More information about the SEC can be found at http://www.sec.gov/.

Tone-at-the-Top – This is another term for entity level controls. Other synonyms are company level controls and control environment.

Transaction – A transaction is an element of a process that will appear in the company financial statements.

Trial Balance - the trial balance is a spreadsheet in which all the balances of each ledger are entered as debit or credit. A trial balance is prepared for each financial period to summarize the closing of the ledger.