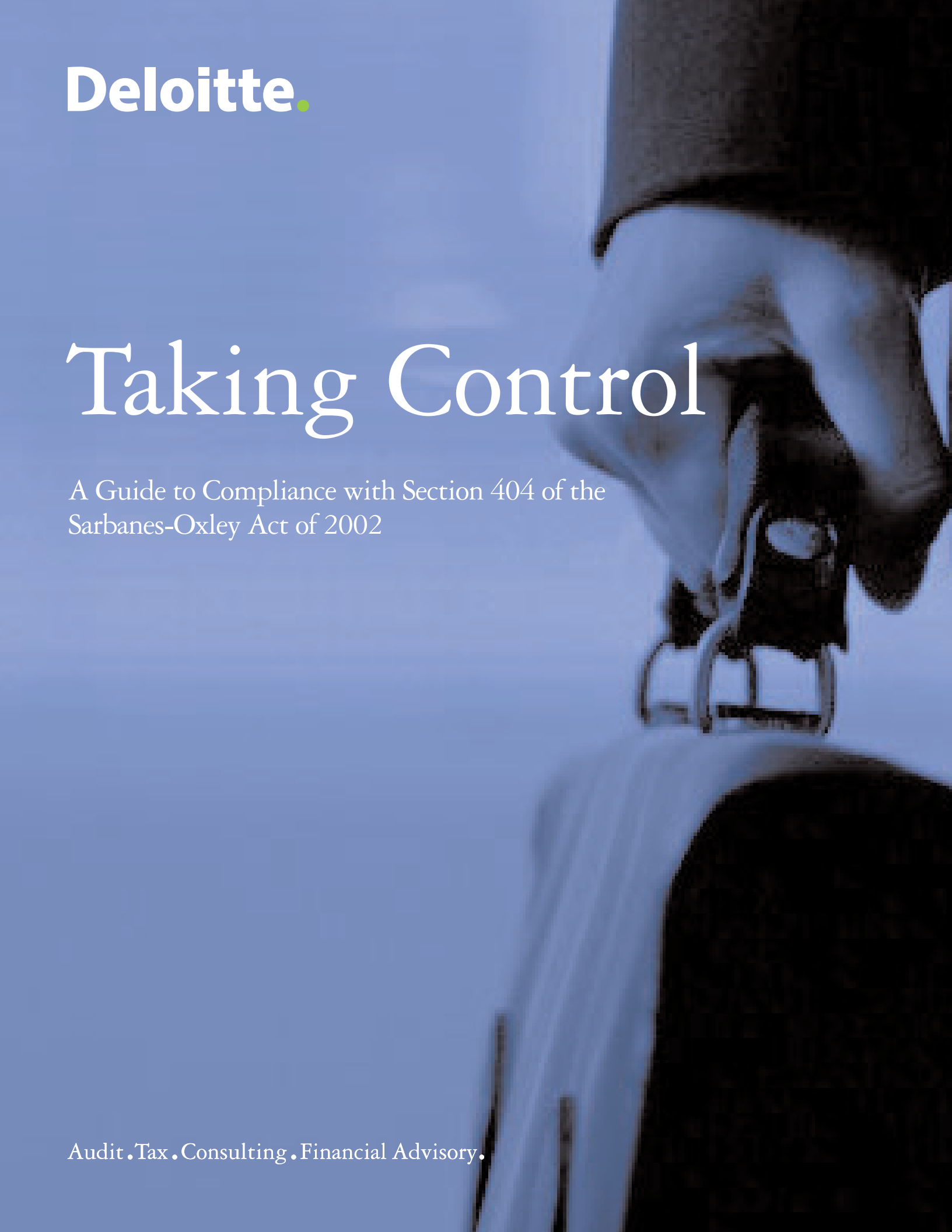
Deloitte.

Taking Control

A Guide to Compliance with Section 404 of the Sarbanes-Oxley Act of 2002



Audit . Tax . Consulting . Financial Advisory .

Table of Contents

Part One: Introduction

If you truly want to "take control" of your section 404 project, education must precede implementation.

1.1 Are You Ready For *Taking Control?*

Establishing a robust system of internal control — one that invokes the intent of the Sarbanes-Oxley Act and all the related Securities and Exchange Commission (SEC) rules and Public Company Accounting Oversight Board (PCAOB) standards — is not a task for the uninformed. If you truly want to "take control" of your Sarbanes-Oxley section 404 compliance effort, education must precede implementation.

In order to get the most out of this publication — and, more importantly, out of your section 404 compliance effort — you need a base level of knowledge. *Taking Control* assumes a certain level of understanding and sophistication on the part of the reader. "Sarbanes-Oxley 101" it's not. As a prerequisite to this document, you should have familiarity with the following:

- SEC's final rules on Sarbanes-Oxley section 404[1]
- PCAOB's auditing standard on Sarbanes-Oxley section 404[2]
- Committee of Sponsoring Organizations of the Treadway Commission's (COSO) *Internal Control — Integrated Framework* publication[3]
- Deloitte & Touche LLP's point of view on Sarbanes-Oxley compliance, *A Bridge to Excellence*[4]
- Deloitte's *Moving Forward* guide to corporate governance and internal control[5]

1.2 How to Read *Taking Control*

Recognizing a diverse readership with varying needs, we have split this publication into four main sections:

1. This **Introduction**
2. The **Executive Overview,** which broadly describes the rationale, objectives, methodology, and philosophy of a well-designed Sarbanes-Oxley section 404 project. Also included are "lessons learned," practical advice gleaned from our field experience in hundreds of Sarbanes-Oxley section 404 projects. Here you'll gain insight into how to properly align and prioritize your project, and will be warned of common pitfalls. Who should read this section? Anyone with responsibility for any facet of a section 404 project, from board members to the leadership team to the project team.
3. The **Implementation Guide,** which provides detailed, step-by-step recommendations for implementing a system of internal control to meet the requirements of Sarbanes-Oxley section 404. Readers of this section should include those directly involved in the section 404 readiness and compliance work. Also, companies that have not yet begun to develop their system of internal control, such as non-accelerated filers and foreign private issuers, may benefit from a cover-to-cover reading of this section. Organizations that are further along with their internal control project may opt to pick and choose cafeteria-style from the material in this section, either to measure their progress or to ensure quality control.
4. The **Appendix,** which contains supplementary information, sample forms, glossary, and reference material.

[1] "Final Rule: Management's Reports on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports," U.S. Securities and Exchange Commission, 2003. Electronic copy can be viewed at: http://www.sec.gov/rules/final/33-8238.htm.
[2] "Release No. 2004-001: Auditing Standard No. 2, An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements," Public Company Accounting Oversight Board, 2004. Electronic copy can be viewed at: http://www.pcaobus.org/rules/Release-20040308-1g.pdf.
[3] "Internal Control — Integrated Framework," Committee of Sponsoring Organizations of the Treadway Commission, copyright 1992, 1994. Executive summary and ordering information for full document available here: http://www.coso.org/publications/executive_summary_integrated_framework.htm.
[4] "Deloitte's Point of View - Sarbanes-Oxley Compliance: A Bridge to Excellence," Deloitte Development LLC, copyright 2004. Electronic copy can be viewed at: http://www.deloitte.com/us/pov. Hard copies also available from your Deloitte professional.
[5] "Moving Forward: A Guide to Improving Corporate Governance Through Effective Internal Control," Deloitte Development LLC, copyright 2003. Electronic copy can be viewed at: http://www.deloitte.com/us/movingforward. Hard copies also available from your Deloitte professional.

Part Two: Executive Overview

If you embrace the spirit of the law — strong ethics, good governance, reliable reporting — you just may get a re-energized company, reassured investors, and maybe even reduced costs.

2.1 A Bridge to Excellence

As you scramble to address the mandates of the Sarbanes-Oxley Act, you may find yourself enmeshed in a process that favors speed over deliberation. The basic work gets done, but at the cost of context and perspective.

Fortunately, while assisting with hundreds of Sarbanes-Oxley section 404 projects, we at Deloitte have gained valuable insights. Here's the most important: *Compliance is not the endgame.*

That's not to say compliance isn't critical, because quite obviously it is. But a much greater reward can be earned by using Sarbanes-Oxley as a bridge to excellence. Your approach holds the key: If you focus on complying only with the *letter* of the law — doing just enough to get by — you may find yourself in a quagmire of bloated controls, burgeoning expenses, and enduring headaches. But if you embrace the *spirit* of the law — strong ethics, good governance, reliable reporting — you just may get a re-energized company, reassured investors, and maybe even reduced costs.

That's right — *reduced* costs. Now, we aren't claiming that your section 404 readiness and compliance work won't be expensive, because surely it will be. But at the same time, if you leverage your compliance effort to include a hard look at business processes and systems, you will almost certainly find unnecessary complexities and redundancies in controls that, if eliminated, can cut costs, sometimes dramatically.

Call it the Sarbanes-Oxley paradox: Wholeheartedly embracing the law can be less expensive than grudgingly accepting it.

2.2 Start with the End in Mind

Meeting the requirements of section 404 of Sarbanes-Oxley is akin to planning a business trip: You can't book your flight until you've chosen your destination. Similarly, you can't plan for section 404 compliance until you know where you're heading. In both cases, you should *start with the end in mind.*

The "end" of the section 404 compliance process arrives when management and the independent auditors issue their reports in the company's annual report. (Of course, "end" is a relative term in this context; in fact, section 404 compliance must be maintained in perpetuity.)

Although the SEC has not scripted the precise language for management's internal control report, the commission has indicated that the report should contain the following:

- a statement *acknowledging your responsibility* for establishing and maintaining adequate "internal control over financial reporting" (for a definition, see Appendix A)
- a statement *identifying the internal control framework* you used to conduct your evaluation of the effectiveness of internal control over financial reporting (which, in most cases, will be the COSO[6] framework)
- an assessment of the effectiveness of your company's internal control over financial reporting as of the end of your most recent fiscal year. (Included here is probably the most critical part of the assertion: *a statement as to whether or not your company's internal control over financial reporting is effective.*)
- disclosure of any "material weaknesses" (see Appendix B for a definition) in your company's internal control over financial reporting. (Note that if there are any disclosed material weaknesses, then you are not permitted to conclude that your internal control over financial reporting is effective.)
- a statement that your independent auditors have issued a report on your assessment of internal control over financial reporting

With the heightened need for good corporate governance, financial reporting integrity and clarity, and information quality — and under the current intense public market and regulatory scrutiny — false, incomplete, or misleading statements may prove problematic. In management's internal control report, you are making representations required and enforceable by law and regulation regarding the effectiveness of your internal control over financial reporting. Care should be taken to get it right.

[6] "Internal Control — Integrated Framework," Committee of Sponsoring Organizations of the Treadway Commission, copyright 1992, 1994. Executive Summary and ordering information for full document available here: http://www.coso.org/publications/executive_summary_integrated_framework.htm.

2.3 The Independent Auditors' Role

While you are busy assessing your internal control over financial reporting, your independent auditors will be working in parallel fashion, evaluating and testing the effectiveness of all five components of the COSO framework. And just as you are required to assess your system of internal control with due diligence, so too are your independent auditors. Thus, they will conduct a vigorous audit of your internal control, encompassing both a telescopic and microscopic view, from the overall control environment to the functioning of specific controls (and all of the other COSO components).

If your independent auditors find everything in order, you'll receive an unqualified opinion on the effectiveness of your internal control over financial reporting and the effectiveness of your assessment process over the same.

But what if your independent auditors identify a material weakness? In that case, instead of an unqualified opinion, you may receive an *adverse* opinion from your independent auditors. Such an outcome could carry considerable negative ramifications.

2.4 Lessons Learned

Deloitte has assisted a variety of companies with section 404 readiness and compliance work. Along the way, we've picked up a wealth of Sarbanes-Oxley-related wisdom, the most important being that your compliance effort must be well-thought-out and executed. We find that in their haste, many companies overlook the things that created the impetus for Sarbanes-Oxley in the first place. Here's a summary of lessons learned:

Get Your Priorities Right

In the course of our Sarbanes-Oxley-related work, we have observed the enthusiasm and eagerness of our clients. Unfortunately, this spirit has sometimes fueled a "fire, ready, aim" approach to section 404 work. Companies understandably want to dive right into documenting, evaluating, testing, and remediating their process-level controls.

While we concur that these tasks form a critical and time-consuming part of any section 404 project, we contend that *they aren't the first steps.* What's needed is not a rush forward but rather a step back — one that gives a broader view and permits careful planning of the project.

Dry Run

To enhance their long-term success, some companies ask their independent auditors to audit the effectiveness of their internal control over financial reporting (or selected pieces of it) prior to the official compliance date. Through this dry run, previously overlooked or undiscovered internal control deficiencies may be identified and remediated in advance, thereby reducing the risk of an adverse opinion once the independent auditors' "official" assessment begins.

Don't allow a "let's-get-it-done" attitude to drive your compliance effort. Conduct your work in a thoughtful way. Pay heed to how you orient, prepare, and enable your teams. Focus on the things that could create a material weakness, such as an ineffective control environment or lack of controls over non-systematic transactions.

As noted earlier, a thorough understanding of Sarbanes-Oxley and COSO is a prerequisite to getting your project done in a proper, timely, efficient, and economical fashion.

Encourage Audit Committee Oversight

The audit committee should be a key player in any effective 404 compliance effort. Indeed, regulatory agencies see audit committee participation as essential: Section 301 of Sarbanes-Oxley requires all exchange-listed companies to have an audit committee, and many private companies have chosen to establish audit committees as well. In addition, your independent auditors will seek evidence of audit committee oversight.

Beyond selecting and supervising the company's independent auditors, the audit committee should review financial reports for completeness and accuracy, and should facilitate discussions among management, the independent auditors, and internal auditors about issues of quality and integrity.

Therefore, you should make sure that the committee's involvement is deep and continuous. Keep members periodically updated. Seek input on areas of project focus. The committee can add real value to the process through objective oversight and seasoned perspective.

Strengthen the Control Environment

Business scandals may have been the impetus for Sarbanes-Oxley, but good governance isn't just about averting the next case of corporate fraud. Rather, it's about leading an organization in the right way: placing proper emphasis on corporate ethics, training employees on their responsibilities for internal control, creating an ethical tone at the top, and providing suitable role models for employees.

Not coincidentally, these are all components of the control environment, which forms the foundation of internal control. The control environment is the universe in which all the other elements exist; it encompasses every aspect of internal control. The control environment provides discipline and structure; encompasses the ethical values and competence of both management and employees; and includes management philosophy and operating style. It embodies the delegation of authority and responsibility; is found in the way management organizes and develops its people; and is seen in the attention and direction provided by the board of directors. The control environment is present in the overall culture of the company, and includes such concepts as attitude, awareness, competence, and style.

Don't let the voluminous rules and standards and the urge to focus on process-level controls obscure the fact that *everything flows from the control environment.* Quite simply, if you haven't established a corporate culture that supports "doing the right thing," then you won't attain good governance.

Across industries and geographies, in companies large and small, certain elements of an effective control environment remain constant. Here are a few:

- *Integrity and ethical values*
  Management should demonstrate an unwavering commitment to character, integrity, and ethical values.
- *Commitment to competence*
  In addition to advancing your business objectives, a knowledgeable, well-trained workforce will also help maintain a strong control environment. Ensure that all employees are aware of the high ethical standards and are not afraid to speak up when something looks strange, unusual, or wrong.
- *Active board of directors/audit committee*
  Revitalize your board with an eye toward highly credentialed, scrupulously

independent members. Today's boards are expected to be active and diligent, to ask the tough questions, and to take swift and appropriate action. Boards should take an active oversight role in the execution of the company's section 404 compliance effort.

- *Management's philosophy and operating style*
  Management's approach toward financial reporting has a strong impact on the control environment. For example, the choice of liberal versus conservative accounting policies sends a message, as does the way non-financial disclosures are handled.
- *Organizational structure*
  The loosely defined organizational structure that was a hallmark of the dot-com era has now been replaced, not necessarily by rigidity and conformity, but rather by a structure that ensures that critical information flows unimpeded.
- *Assignment of authority and responsibility*
  Those charged with maintaining an effective system of internal control should have: job descriptions that are clearly delineated, a full understanding of their responsibilities relating to internal control, sufficient knowledge and experience to carry out their internal control-related duties competently, and the resources and the authority to get the job done.
- *Human resource policies and practices*
  Hiring and retaining quality employees should be a high priority. Provide abundant professional development opportunities. Include internal control and business ethics in employee evaluations, and make compensation and promotions contingent upon these evaluations.

Integrate Your IT Group

Few companies could operate in today's business environment without complex information systems. In addition to providing critical support to your business, these systems also form a linchpin of your company's system of internal control. Indeed, IT controls are fundamental to compliance with section 404.

Thus, it is critical to integrate your IT professionals in your section 404 compliance effort. The complexity of the IT control issues and the specialized expertise required to define, develop, and implement effective solutions for identified deficiencies demand the participation of your IT managers. Involve them in the planning and execution phases from the outset.

Consider IT Controls

Your section 404 project provides an opportunity to look at your manual controls with a fresh eye to determine if they are optimally appropriate, efficient, and effective. Manual controls are pervasive in many companies because they are easier to understand, implement, and test. Yet oftentimes, manual controls can be replaced with IT controls that provide better efficiency and results.

Consider the control areas of segregation of duties and authorization. When invoice payments are processed, access to the software application can be configured so that only authorized users are able to make payments. Approvals of purchase orders and payments can also be segregated through IT controls. Similarly, when journal entries are processed, user access can be configured so that only authorized members of staff may post journal entries for stipulated amounts, particular divisions, etc.

If you apply a similar critical analysis to all your manual controls, you can simultaneously root out inefficiencies and strengthen your system of internal control.

Consult With Your Independent Auditors

Your independent auditors are required by law to maintain independence and professional skepticism, but that does not imply an adversarial relationship. After all, you share plenty of common ground — most notably the desire for reliable financial reporting!

Thus, you should be talking to your independent auditors at every step of your section 404 compliance effort. It is never too early to begin the dialogue. Conversations during the scoping and planning phase can ease your tasks further along. You should agree on timeframes and milestones. You should ensure that your definitions of materiality are in alignment.

Make sure your independent auditors understand the nature, scope, and timing of your control testing, as well as who is performing the testing. Collaboration will enable your independent auditors to use your work to the fullest extent possible.

So talk early and often. Remember, your independent auditors have likely been engaged in many more section 404 projects than you have. You are paying for that expertise — so make the most of it!

Don't Neglect Other COSO Components

Out of a desire to get their section 404 compliance efforts moving forward rapidly, many companies focus heavily on process-level controls. This is understandable, as these controls represent tangible, easy-to-understand components of internal control.

But section 404 calls for an assessment of *all* the components of internal control. Under the COSO framework, this includes not only control activities, but also controls over the control environment, risk assessment, information and communication, and monitoring.

Focusing exclusively on control activities will result in an assessment that is only partially complete, and that could create problems. If you haven't covered all the components of COSO, then your assessment will lack sufficient basis for determining that your internal control is effective.

Risk assessment, for example, is a critical COSO component that is sometimes neglected entirely or documented as an afterthought. Yet understanding and documenting risks to reliable financial reporting is essential to evaluating the adequacy of controls. So be sure to work risk assessment into your project plan, with special attention paid to high-risk areas, including complex transactions or those involving significant judgment; also focus on risks related to fraud and safeguarding of assets.

Understand Fraud

No system of internal control, however well-designed, can prevent all acts of fraud. But there is plenty you can do to deter, impede, discourage, and detect corporate misdeeds.

The first step involves understanding fraud. What, exactly, is financial statement fraud? The American Institute of Certified Public Accountants (AICPA) refers to financial statement fraud as "an intentional act that results in a material misstatement in financial statements that are the subject of an audit."[7] However, others expand the definition to include the notion that financial statement

[7] AICPA. (2002). *Statement of Auditing Standards (SAS) No. 99. Consideration of fraud in a financial statement audit.* New York.

fraud is usually conducted by management or with their consent and knowledge. Thus, Elliott and Willingham describe financial statement fraud as "the deliberate fraud committed by management that injures investors and creditors through materially misleading financial statements."[8]

After understanding comes analysis. Where is your company most vulnerable? Does the part-time assistant to the accounts payable clerk have the ability to bring down the company? Probably not. Instead, focus on the high-risk areas, such as the following:

- management override
- manual journal entries
- estimates
- rationale for significant transactions
- disclosures in financial statements (and, perhaps more importantly, disclosures *not* in the financial statements)
- selection and application of accounting principles

Exploit Technology

The more deeply you embed internal control into your corporate culture and into the daily routines of your business, the more effective, sustainable, and efficient your program will become. One of the best ways to attain this integration is through the intelligent deployment of technology. While no panacea, information technology can play a critical role in sustaining your compliance efforts.

For many companies, the early work of control documentation has typically been performed using existing simple applications (word processing, spreadsheets, or Web-based programs). However, more robust technology may be required to sustain a company-wide rollout and the ongoing evaluating, testing, and reporting necessary to support your section 404 assessment procedures. Many software vendors and consulting companies have developed software in this area.

Finding the right technology to support your Sarbanes-Oxley efforts will depend on a number of factors, including:

- your current functional requirements for section 404
- additional or future requirements (other regulatory compliance, internal audit, enterprise risk management)
- your information technology infrastructure (i.e., the technology currently supported by your IT organization). Your CIO should play an active part in the technology decision.

Be Smart About Testing

When it comes to testing your controls, there are no specific standards for the number of selections nor the types of tests to be conducted. Factors such as the role of the tester, the nature of the control, and the frequency of the control's use will all come into play. Controls that are executed infrequently (annually or quarterly) may require a limited number of transactions to test. Controls in frequent use may require dozens of selections to verify their effectiveness. But irrespective of how many selections you make, you are responsible for obtaining at least the same level of assurance[9] as your independent auditors, so consult with them early in the process.

Define a Process for Handling Deficiencies

Even the best-run companies will have internal control deficiencies. A properly designed section 404 project will attempt to identify and remedy all internal control deficiencies before the end of the fiscal year. (Nonetheless, some internal control deficiencies may still exist at year end.)

But how do you deal with these internal control deficiencies once you identify them? You handle them according to the protocols outlined in your *control internal control deficiency governance process.*

Early in your project planning, you should develop and implement detailed steps for handling internal control deficiencies. The benefits of this process will be many, including consistency in addressing and remediating internal control deficiencies; independent auditors' concurrence on internal control remediation methodology (which may avoid surprises later!); more clearly defined responsibility for addressing internal control deficiencies; improved decision-making regarding internal control-related changes in the business; enhanced sustainability (an important element of a good control environment); and improved communication to ensure that issues are considered and addressed.

Items to define in your internal control deficiency governance process will include responsibility (by name or job title), timing (what is the timeframe for addressing the internal control deficiency?), notification/communication (who needs to know about it?), and documentation (where and in what form is the information recorded?).

You should also include criteria for determining the proper classification of internal control deficiencies (internal control deficiency, significant deficiency, or material weakness). See Appendix B for a definition of these terms — and discuss them with your independent auditors. Since your independent auditors will also be evaluating your internal control deficiencies, you need to reach an agreement on your internal control deficiency classification process. Early attention to this issue will save you time later.

Consider the Impact of Changes to Your Business

Mergers and acquisitions represent an important feature of the American business landscape. Yet before you consummate any deal, you should be aware of the impact that M&A activity — or any other significant changes to your business structure or operations — can have on compliance with Sarbanes-Oxley. Essentially, once you acquire another company, that entity's system of internal control becomes your own, and you become responsible for its internal control over financial reporting. Fortunately, the SEC has acknowledged that it may be difficult to conduct an assessment of an acquired company's internal control over financial reporting in the period between the acquisition date and the date of management's assessment. In such cases, the acquired company may be excluded from management's report on internal control over financial reporting. However, this exclusion must be noted in the report as well as disclosed on Form 10-K or 10-KSB. Furthermore, you may only omit an assessment of an acquired company's internal control over financial reporting for a period of no more than one year from the date of acquisition, and from no more than one annual management report on internal control over financial reporting. Other restrictions and provisions apply. Consult your independent auditors for additional details.

[8] Elliott, R.K., and Willingham, J.J. (1980). *Management fraud: Detection and deterrence.* New York: Petrocelli Books.
[9] As defined by the PCAOB, reasonable assurance *"includes the understanding that there is a remote likelihood that material misstatements will not be prevented or detected on a timely basis. Although not absolute assurance, reasonable assurance is, nevertheless, a high level of assurance."* Source: "Release No. 2004-001: An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements," Public Company Accounting Oversight Board, 2004.

The Cost of Compliance

A survey of 321 companies, published by Financial Executives International (FEI) in February 2004, showed that businesses with more than $5 billion in revenue expected to spend an average of $4.7 million implementing Sarbanes-Oxley section 404 in the first year of compliance. Costs included consultants, lawyers, auditors, and new software. Some of these costs, most notably hardware and software systems, will decrease after the first year. But other costs, such as paying independent auditors to assess internal control, are expected to stay constant. Companies in the FEI survey expect those fees to be $1.5 million annually.

FAQs from CXOs

The technical and logistical hurdles posed by Sarbanes-Oxley section 404 have raised anxiety levels in the business world. Many executives are uncertain that they are proceeding properly and are worried whether they are focusing and aligning their project appropriately with the law's requirements. Our Deloitte professionals have fielded many queries in this regard. Here are some of the questions asked and answered most frequently:

Do we have the right competencies to get our section 404 project done?
Chances are you have more internal talent at your disposal than you realize. While resource requirements will differ based on factors such as company size, industry, geography, and other variables, generally speaking, you will need to draw on individuals from tax, human resources, information technology, finance and accounting, internal audit, and operations. You should be aware that many of these people have never considered themselves as part of the financial reporting infrastructure. But today, under Sarbanes-Oxley, virtually everyone is!

Section 404 compliance is a huge undertaking. How will I ever get it done on time?
One of the most productive steps you can take is to get your independent auditors involved immediately. If you conduct your section 404 project in consultation with your independent auditors, you should avoid surprises on either side. Also, the sooner your independent auditors start the assessment procedures, the more time you will have to remediate any internal control deficiencies they find. And finally, you should carefully prioritize your activities; in essence, do a risk assessment of your section 404 project. Focus on the things that could create a material weakness, such as an ineffective control environment or lack of controls over non-systematic transactions.

How do we sustain this program so we remain in compliance?
Compliance with Sarbanes-Oxley section 404 is not a "once-and-done" effort. Because the evaluation, testing, and reporting requirements recur on an annual basis, you must sustain your compliance indefinitely. Therefore, you should build an efficient and effective compliance infrastructure that enables repeatable, reliable actions. Focus on educating your employees, optimizing your business processes, deploying information technology, and communicating openly.

Part Three: Implementation Guide

Remember: Your objective is simple. You are working to attain reliable financial reporting for your company.

3.1 The Practical Pages

In contrast to the high-level perspective provided in the *Executive Overview*, this *Implementation Guide* section provides a ground-level vantage point. Over the coming pages, you will receive straightforward guidance for implementing a COSO-based system of internal control.

Use this section in the manner that best suits your needs and purposes: either a complete front-to-back reading to become fully versed in the subject, or an *a la carte* sampling to selectively enhance your knowledge, jumpstart your work, benchmark your progress, or troubleshoot your project.

3.2 Why You Should Read This Implementation Guide

If you're feeling intimidated by the sheer bulk of this section, consider:

- Deploying COSO is a detailed process; there are simply no shortcuts or workarounds. Hence the heft of this section.
- *Taking Control* is not a rehash of the COSO publication. Rather, it offers a step-by-step approach that draws upon the detailed knowledge, leading practices, and cumulative experience of our practitioners and clients — men and women who have spent thousands of hours in the field assisting with the implementation of systems of internal control based on COSO.
- Building or strengthening a system of internal control sturdy enough to satisfy the requirements of Sarbanes-Oxley section 404 is painstaking, time-consuming, and expensive. Yet as distasteful as that sounds, the alternative — coming up short in your compliance efforts — could be significantly worse.

3.3 Keep It Simple

To say that Sarbanes-Oxley section 404 has created a tumult in the business community may be an overstatement, but not by much. From the board room to the shipping dock, executives and workers are grappling with new demands, more oversight, heightened responsibility, and increased pressure. Costs are mounting, deadlines are approaching, and sanctions are looming for those who don't get it right.

But when things seem overwhelming, stop for a moment. Take a deep breath. Relax. Remember: Your objective is simple. You are working to attain *reliable financial reporting* for your company.

With this goal in mind, you should be able to ask yourself at any point in your section 404 project, *How does this particular task help improve the reliability of my financial reporting?* If you can clearly trace the task at hand back to your overriding objective — reliable financial reporting — then the entire project will come into better focus, and its disparate elements will unite into an understandable whole.

3.4 Build the Foundation

Before you frame the first wall, you have to construct the foundation. Mucking around in the trenches isn't the glamour work, but nothing else can be supported until you do.

The Middle Market Dilemma

Of all businesses struggling with Sarbanes-Oxley section 404 implementation, perhaps the most untenable position is that of middle-market companies. Human resources are stretched thin, with most employees already working at capacity. A tough economy and ongoing financial constraints preclude lavishing money on outside consultants to shepherd the project. Just attending to the day-to-day business of the company is difficult enough, never mind taking on a new, labor-intensive, cost-prohibitive project.

How to cope? Well, this publication provides a good place to start. Take our advice to heart. Get your priorities straight. Keep your project simple. Leverage existing technology, such as pre-populated templates. Identify an internal control champion within your firm. Conduct training workshops. Re-read COSO. And communicate tirelessly about good governance and internal control.

The same principle applies to your section 404 project. Here's a checklist of preliminary activities you'll need to address before you can proceed to the more heady stuff. (If you need more detail on any particular item, see Deloitte's *Moving Forward* publication, referenced previously.)

- document your business operations (locations, units, and subsidiaries; partnerships, shared services, and extended enterprises; etc.)
- create a repository containing copies of corporate codes, procedures, policies, manuals, charts, and descriptions
- inventory and record pension plans, stock option plans, compensation packages, and profit-sharing plans
- establish a steering committee
- deploy a disclosure committee
- create an internal control project team
- form a program management office
- determine the role of internal audit
- consult with your independent auditors
- confer with senior management, disclosure committee, audit committee, and the board of directors
- determine the role of information technology
- train the project team
- develop your section 404 project work plan and your project budget
- select appropriate technology

3.5 Scope the Project

At this stage of your section 404 project, you'll be defining the parameters of your work, including identifying important locations, significant accounts, and key business processes. Essentially, you'll be determining which parts of your business have a significant impact on internal control over financial reporting, and which parts don't. The former will be "scoped in" to your section 404 internal control assessment; the latter will be "scoped out."

Determine Objectives to Include in the Project

COSO is a principles-based framework that is composed of three objectives: effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations. Any section 404 project should, naturally, focus on the financial reporting objective. However, your project team may wish to consider including the other objectives — efficiency and effectiveness of operations and compliance with applicable laws and regulations — in its section 404 readiness project. By focusing on all the objectives, your company can drive better business performance. And, as noted earlier, by treating the requirements of section 404 as an opportunity, rather than a burden, your company may reap dividends far beyond compliance alone.

In some cases, you will have no choice but to include elements of the two other COSO objectives, because they sometimes overlap with internal control over financial reporting. For example, in the realm of efficiency and effectiveness of operations, consider a telephone company's switching operations. If these switches function to route and record customer calls, which in turn provides the basis for invoicing, then switching operations should be considered part of financial reporting and thus subject to section 404.

With respect to compliance with applicable laws and regulations, it is clear that following the laws, rules, and standards related to Sarbanes-Oxley section 404 is directly related to the preparation of reliable financial statements. But other laws and regulations will also come into play. For example, internal control over financial reporting would include controls over the computation of taxes, because tax liability has a direct and, usually, material effect on the financial statements. (However, the processes and controls to prepare and file tax returns would not be included, as these activities don't have a direct bearing on the financial statements.)

Other examples of laws and regulations that may have a direct and material effect on the financial statements may include the recognition and/or disclosure of certain employee benefit-related matters, such as payroll taxes or retirement benefits, and industry-specific laws and regulations, such as those directly affecting financial reporting for governmental contractors, banks, or health care providers.

Internal Control Over Financial Reporting: A Primer

Before you can effect internal control over financial reporting, you must understand the term itself, including its scope and limits. In its final rule,[10] the SEC provided a detailed definition, which may be found in Appendix A.

The gist of the definition is contained in the SEC's interpretation that internal control over financial reporting covers "the applicable laws and regulations directly related to the preparation of financial statements."

The SEC's definition of internal control over financial reporting includes policies and procedures that:

(1) pertain to the maintenance of records that in reasonable detail accurately and fairly reflect the transactions and dispositions of the assets of the registrant.

Although maintenance of records may be thought of as a state or condition as opposed to a control objective, there's another way to look at it: The *absence* of appropriate records may impair the effectiveness of the persons responsible for performing control activities. Thus, you should ensure that adequate records are maintained not only for your routine transactions (e.g., payroll), but also for non-routine events and transactions (e.g., support for estimates, journal entries, and the selection and application of new accounting principles).

Additionally, maintenance of records also includes that portion of business continuity or disaster recovery related to the controls over maintaining back-up and data recovery.

Also, although your company's record retention policies (i.e., how long you retain your financial records in storage) appear to be a legal consideration that falls outside the scope of section 404, it is advisable to maintain such records in a manner similar to the maintenance of records that support the financial statements.

(2) provide reasonable assurance that … receipts and expenditures of the registrant are being made only in accordance with authorizations of management and directors of the registrant.

Each of the five components of COSO will have areas in need of controls related to authorization, including the following:

- Control Environment: assignment of financial authority by the board of directors to executive and middle management; related party transactions; expense accounts and perquisite arrangements; executive management compensation arrangements (including incentive-based arrangements)
- Risk Assessment: identifying any significant risks involving the ability of an employee to initiate and/or process unauthorized transactions

[10] "Final Rule: Management's Reports on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports," U.S. Securities And Exchange Commission, 2003. Electronic copy can be viewed at: http://www.sec.gov/rules/final/33-8238.htm.

- Information and Communication: communication of authority across the organization; controls in the IT systems to prevent unauthorized access
- Control Activities at the Process/System Level: authority for specific types of transactions within each process
- Monitoring: monitoring for unauthorized transactions (e.g., unauthorized journal entries)

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

This means that controls over fraudulent activity are intended to prevent or detect unauthorized expenditures or investments, unauthorized incurrence of liabilities, stolen inventory, the conversion of assets to personal use, and other illegal activities.

Determine Materiality

"Materiality" is a term used to describe the significance of financial statement information to decision-makers, such as shareholders. An item of information is considered material if it is probable that its omission or misstatement would influence or change a decision of these stakeholders.

In its Statement of Financial Accounting Concepts No. 2, the FASB stated that "the omission or misstatement of an item in a financial report is material if, in the light of surrounding circumstances, the magnitude of the item is such that it is probable that the judgment of a reasonable person relying upon the report would have been changed or influenced by the inclusion or correction of the item."[11]

But as Shakespeare might say, "Ay, there's the rub." Because determining exactly what kind of information or how many dollars it would take to sway an investor is a tricky process dependent on subjective interpretation.

Yet materiality is critical to effective internal control over financial reporting. Materiality is calculated because it enables management to classify internal control deficiencies into the categories of material weaknesses, significant deficiencies, or internal control deficiencies. (For a definition of these terms, see Appendix B). It is also used to determine which accounts and disclosures are significant (discussed in greater detail below).

So how does one determine materiality? The AICPA suggests that financial impact on after-tax income may be one appropriate measure: "… it is generally recognized that after-tax income from continuing operations is, in most circumstances, the measure of greatest significance to the financial statement users of entities whose debt or equity securities are publicly traded."[12]

The group says that other significant accounts of the financial statements — current assets, net working capital, etc. — can be reasonably selected as well. But regardless of what is chosen, "in all instances, the element or elements selected should reflect, in the auditor's judgment, the measures most likely to be considered important by the financial statement users."[13]

But note, too, that materiality cannot be reduced to a simple numerical formula. A thorough assessment of materiality requires that the facts be considered in the context of the surrounding circumstances. Thus, qualitative factors, which also consider the needs of a "reasonable person," should be weighed as well, including items that:

- represent related-party balances and transactions
- change a loss into a profit or vice versa
- mask a change in earnings or other trends
- hide a failure to meet analyst expectations
- affect compliance with loan and other covenants
- increase executive compensation

The SEC states that "The use of a percentage as a numerical threshold, such as five percent, may provide the basis for a preliminary assumption that — without considering all relevant circumstances — a deviation of less than the specified percentage with respect to a particular item on the registrant's financial statements is unlikely to be material. The [SEC] has no objection to such a 'rule of thumb' as an initial step in assessing materiality. But quantifying, in percentage terms, the magnitude of a misstatement is only the beginning of an analysis of materiality; it cannot appropriately be used as a substitute for a full analysis of all relevant considerations."[14]

Every company is unique, and the methods of determining materiality and results of that determination will vary accordingly. As always, discuss your conclusions and your methodology with your independent auditors and audit committee. And be sure to document your decisions.

More on Materiality

- While you should not base your materiality decisions on the materiality levels set by your independent auditors for purposes of the internal control audit, you should nonetheless discuss the matter with them in advance. It would be unfortunate to set your own materiality at a level higher than what your independent auditors will use to conduct their procedures because they may conclude that your assessment process is not effective because it was not sufficiently inclusive.
- The quantitative component of your materiality is a moving target. You should revisit your materiality calculation at least on an annual basis, and more frequently if conditions and circumstances dictate.
- Companies tend to focus on the financial statements when setting materiality. They often forget that non-numerical disclosures (in footnotes to the financial statements) also play a large role in influencing a "reasonable person."

[11] FASB, Statement of Financial Accounting Concepts No. 2, Qualitative Characteristics of Accounting Information ("Concepts Statement No. 2"), 132 (1980).
[12] "Interpretations of SAS No. 47 (AU Section 312)." American Institute of Certified Public Accountants. Electronic copy can be viewed at: www.aicpa.org/members/div/auditstd/announce/interpretations.htm.
[13] Ibid.
[14] "SEC Staff Accounting Bulletin: No. 99 - Materiality," U.S. Securities and Exchange Commission, 1999. Electronic copy can be viewed at: http://www.sec.gov/rules/acctrps/sab99.htm.

Identify Significant Locations or Business Units

In your preliminary activities, you took a comprehensive inventory of all your locations and business units. Now, you will whittle the list down to the most critical of these sites. Your objective is to separate the insignificant — those locations or businesses that could not create, either individually or in the aggregate, a material misstatement in the financial statements — from the significant.

Using the definitions of materiality that you have developed, methodically examine each location or business and evaluate the relative financial significance and the risk of material misstatement arising from it. Consider that some sites may have unique or specific risks that, by themselves, could create a material misstatement. Also remember that some locations or business units in isolation may seem immaterial, but in combination may attain a level of financial significance that could create a material misstatement in the financials.

In most cases, the business units and locations identified should represent a large portion of the company's total operations and financial position. Determining "large portion" is a matter of judgment, which should be discussed with your independent auditors since the number of locations selected by the company should be generally more than that the number selected by your independent auditors.

As always, document your work and the criteria you used.

Identify Significant Accounts

With significant business units identified, it's time to examine the financial statements from each to determine significant accounts.

What constitutes a significant account? Perhaps a more appropriate question would be, what doesn't? It's only slight hyperbole to state that *every* account could be considered significant.

Your materiality definition will be the ultimate determining factor. If the account balance or financial statement line item is sufficiently large — individually or in the aggregate — that an error or misstatement within it could have a material effect on the financial statements, then it should be identified as a significant account.

Of course, financial statement line items are often comprised of multiple general ledger accounts. Within each of those financial statement line items, account balances should be determined by a two-step process: first, aggregate general ledger accounts that have similar risks and share common processes and controls; second, disaggregate into components those financial statement line items and general ledger balances that have differing risks and controls. Then, at this component level, account balances above the materiality level (considering the risk of both overstatement and understatement) should be identified as a significant account.

Assuming that a $700,000 materiality level has been established for identifying significant accounts, the charts below illustrate the process:

Figure 1.1

Financial Statement Line Item Level[1]	Account Balance	Significant?
Cash	$ 2,000,000	Yes
Accounts Receivable	$ 6,000,000	Yes
Inventory	$ 7,000,000	Yes
Other Assets	$ 1,000,000	Yes
Property, Plant & Equipment	$ 800,000	Yes
Prepaid and Other Current Assets	$ 400,000	No[2]
Payables - Related Party	$ (100,000)	Yes[3]
Derivative Liability	$ (400,000)	Yes
Accounts Payable	$(3,000,000)	Yes
Accrued Liabilities	$(2,000,000)	Yes
Long-Term Debt	$(5,000,000)	Yes
Stockholders' Equity	$(6,700,000)	Yes

(1) For this illustration, only the single-location balance sheet has been depicted to identify the significant accounts at the financial statement level. However, the income statement, cash flow statement, and footnote disclosures also should be included.

(2) The line item is less than the threshold and, for illustrative purposes, it does not contain qualitative factors that would cause the line item to be deemed significant.

(3) Although less than the threshold, for illustrative purposes, the line item is identified as significant because of significant qualitative considerations.

Figure 1.2

Account Balance Level	Account Balance	Significant Account?
Accounts Receivable:		
Trade Accounts Receivable	$ 4,600,000	Yes
Related Party Receivables	$ 400,000	Yes[4]
Miscellaneous (10 @ $100,000)	$ 1,000,000	No[5]
Total	$ 6,000,000	

(4) Although less than the threshold, for illustrative purposes, the account is identified as significant because of significant qualitative factors.

(5) For illustrative purposes, assume that the 10 miscellaneous accounts of $100,000 each are not subject to the same risks and controls and that there are no significant qualitative factors. These accounts individually would not constitute significant accounts and, thus, these accounts are not considered significant accounts. Because they exceed the threshold in the aggregate, the key control(s) should be evaluated.

Scoped Out and Forgotten?

Caught in the whirlwind of identifying important locations and significant accounts, companies sometimes forget about those they have left behind — the items that have been "scoped out" of their section 404 project. Many companies have the mindset that if the location or account doesn't have a significant impact on internal control over financial reporting, then no controls are needed. This, we contend, is an inadvisable stance. Indeed, companies with a reputation for good governance and strong internal control have long realized the need for controls at **all** their business locations and for **all** their accounts. The benefits include standardization and simplification; an improved overall control environment; and easier transitions due to expansion or other changes in the business. Scoped in or scoped out, internal control should be ubiquitous. It's just good business.

Additionally, other account balances that are less than the threshold also may be identified as a significant account taking into consideration qualitative factors, such as the expectations of a reasonable user. For example, investors might be interested in a particular financial statement account even though it falls below the threshold because it represents an important business performance yardstick.

The PCAOB offers this definition of account significance:

An account is significant if there is more than a remote likelihood that the account could contain misstatements that individually, or when aggregated with others, could have a material effect on the financial statements, considering the risks of both overstatement and understatement. Other accounts may be significant on a qualitative basis based on the expectations of a reasonable user. For example, investors might be interested in a particular financial statement account even though it is not quantitatively large because it represents an important performance measure.

Note: For purposes of determining significant accounts, the assessment as to likelihood should be made without giving any consideration to the effectiveness of internal control over financial reporting.[15]

Identify Relevant Assertions for Each Account

Financial statement assertions are representations by management regarding the completeness, validity, and accuracy of financial statements. Assertions can be broadly classified as follows:[16]

- *Existence or Occurrence* — Assets, liabilities, and ownership interests exist at a specific date, and recorded transactions represent events that actually occurred during a certain period.
- *Completeness* — All transactions and other events and circumstances that occurred during a specific period, and should have been recognized in that period, have, in fact, been recorded.
- *Valuation or Allocation* — Asset, liability, revenue, and expense components are recorded at appropriate amounts in conformity with relevant and appropriate accounting principles.
- *Rights and Obligations* — Assets are the rights, and liabilities are the obligations, of the entity at a given date.
- *Presentation and Disclosure* — Items in the statements are properly classified, described, and disclosed.

Note that assertions are not mutually exclusive; thus, more than one of these assertions can be applied to the significant accounts and disclosures. Take, for example, accounts receivable. Relevant assertions would include "existence or occurrence" (recorded accounts receivable exist and are recorded accurately); "completeness" (all accounts receivable have been recorded); "valuation" (accounts receivable are collectable); "rights and obligations" (the company has legal claim to the accounts receivable); and "presentation" (accounts receivable are properly displayed and classified on the balance sheet with appropriate footnote disclosures).

Since you have already identified your significant accounts and disclosures, work methodically through them and assign relevant assertions to each.

Identify Significant Processes

"Significant processes" are the procedures that underlie your account balances, the actual real-world steps that employees undertake to initiate, record, process, and report transactions. Significant processes that affect financial reporting may include taking inventory, processing payroll, reconciling bank accounts, making journal entries, aging accounts receivable, and myriad other day-to-day activities involved in running a business.

To identify significant business processes, follow these steps.

Identify the major classes of transactions for each significant account.
Major classes of transactions are identified by considering the account activity (e.g., the debits and credits) within the significant account. Three types of transactions are possible: routine, non-routine, and periodic. Routine transactions are those that occur frequently and are expected in the ordinary course of business. For example, in manufacturing environments, the routine types of transactions that may occur include (1) distributor sales, (2) direct customer sales, and (3) Internet sales.

Non-routine transactions are those that occur infrequently. Examples of non-routine transactions include transactions with special terms; mergers, acquisitions, and divestitures; plant closings; extraordinary items; and disposals of a segment of a business.

Periodic transactions are those that occur at points in time and generally as part of the month-end, quarter-end, and annual closing processes. These may include the accrual of accounting estimates, the calculation of income taxes, and other accruals (e.g., interest on investments and debt, and accrued liabilities).

To illustrate, let's use accounts receivable as a sample significant account. Within this account, the major classes of transactions may include sales, sales returns, cash receipts, write-offs, and journal entries. These classes may be determined to be "major" due to their financial significance (such as sales and returns), importance to the closing process (journal entries), or levels of subjectivity (write-offs).

[15] "Release No. 2004-001: Auditing Standard No. 2, An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements," Public Company Accounting Oversight Board, 2004.
[16] "Statement of Accounting Standard (SAS) No. 31," American Institute of Certified Public Accountants.

Identify the significant processes supporting the major classes of transactions. Processes may be categorized into two major types: transaction-level processes and company-level processes. Transaction-level processes involve individual transactions. These may be *systematic* (automated) processes such as sales activity, billing, collection, and payroll. Or they may be *nonsystematic* (manual) processes, such as intangible assets, allowance for sales returns, allowance for doubtful accounts, and litigation reserves.

Company-level processes involve financial reporting and closing, including such activities as journal entries, reconciliations, and consolidation. Company-level processes should always be considered significant.

Thorough documentation of significant processes provides a better understanding of the company's system of internal control over financial reporting, which will aid both the internal team and the independent auditors in their work and will aid in the identification of control objectives and risks (which will be discussed later in this document).

Identify Significant Application Systems

A significant software application system has an important impact on financial reporting because, among other characteristics, it processes major classes of transactions.

Identifying significant software application systems is a fairly straightforward process: Once you have identified the significant business processes (as described above), match them to the software applications that support those processes.

Identify the Computer Processing Environment

A computer processing environment is a location that supports computer hardware and software. It is possible to have multiple computer processing environments at one physical location. A distinguishing feature of the computer processing environment is its unique combination of operating procedures and programmed controls. A computer processing environment also includes those individuals who support the computer processing, but who may not be physically located in the same location. For example, a company might have a single data center (i.e., processing location) that includes both a mainframe computer and one or more smaller computers. Because the operating procedures and programmed controls differ significantly between the mainframe and the smaller computers, you should treat them as separate computer processing environments.

Identify Service Organizations and Other Extended Relationships

Many companies outsource business processes, including manufacturing, order fulfillment, payroll, accounting, human resources, shipping, tax reporting, coupon and warranty processing, and other functions. As part of your scoping process, you should identify all of these relationships because, depending on the nature of each, you may be responsible for evaluating and testing the controls within some of these organizations.

In your assessment process, you should include any outside organization that is part of your information system. An outside organization is part of your information system if the services it provides or the transactions it performs affect any of the following:

The classes of transactions in your operations that are significant to your financial statements. Thus, only service organizations (including IT application and general computer controls) that impact a company's major classes of transactions, significant accounts, or processes need to be considered.

The procedures, both automated and manual, by which transactions are initiated, recorded, processed, and reported from their occurrence to their inclusion in the financial statements. Procedures in any of these four stages may be outsourced. Oftentimes the processing stage activities may be outsourced, while the company performs the initiation, recording, and reporting activities.

The related accounting records, supporting information, and specific accounts in your financial statements involved in initiating, recording, processing, and reporting transactions. For example, accounting records, such as payroll registers or health care claims disbursement records, may be maintained by the service organization on behalf of the company.

How your information system captures other events and conditions that are significant to the financial statements. Examples include (1) data provided by an outsourced manufacturer to assist the company in the identification of inventory adjustments or write-downs of inventory located at the outsourced manufacturer, and (2) securities pricing services used by financial organizations to "mark-to-market" its investment portfolio.

The financial reporting process used to prepare your financial statements, including significant accounting estimates and disclosures. This may range from the involvement of third parties in assisting management in the preparation of estimates (such as fair value, actuarial, or environmental) to the outsourcing of the entire financial reporting process, including the period-end closing and reporting processes.

It is important to distinguish between service organizations and vendors because service organizations are "scoped" into the company's assessment of internal control over financial reporting while vendors are not. One key factor that can aid in the distinction: If your company includes transactions or events that are processed by a service provider in your own financial statements, then it is likely that the service provider represents a service organization. Consult with your independent auditors if you have any questions.

3.6 Establish Objectives and Identify Risks

Your company faces continual risks. On the broadest level, competitive risks can threaten the very survival of your organization. On a less monumental scale, internal risks can affect your petty cash balances or even your supply of mechanical pencils. The point is that your company faces risks from all quarters, some significant, some mundane.

Of course, risk management is a broad topic. In the context of Sarbanes-Oxley section 404, it is narrowed: Risk is an event or condition that can negatively affect the ability of the organization to produce timely and reliable financial reporting.

Risk assessment is inextricably linked to the scoping process described above. As you determined materiality and then identified

Focus on Fraud

Section 404 of Sarbanes-Oxley requires companies to include an assessment of fraud risk, which can arise from a variety of places and be attributable to a number of causes. For example, management override has been a significant factor in several highly publicized fraud cases. Revenue recognition can be another area ripe for abuse, since the rules governing revenue are often misapplied. Fraud risk can manifest itself in the control environment as well, if, for example, management applies strong pressure on employees to show short-term earnings. Executive incentives can also backfire: Management compensation that is contingent upon corporate performance can provide strong temptation to "cook the books."

Here are a few additional observations on fraud:

- The benefits of an anti-fraud program to an organization are not limited only to reduced costs. Under the Federal Sentencing Guidelines, there is up to a 95 percent reduction in penalties for companies that have implemented programs to prevent and detect any violations of law.
- The cornerstone of an anti-fraud environment is a culture founded on honesty and integrity, reflected by the formal and informal organizational code of conduct and actual and perceived adherence to that code. Built on that foundation, an effective anti-fraud program includes a comprehensive assessment of the organization's fraud risks and an enterprise-wide risk monitoring program specifically designed to determine the effectiveness of preventive and mitigating anti-fraud controls.
- The fraud risk assessment should include the individuals with day-to-day involvement in the significant processes being assessed. For example, an assessment of the risks inherent in a revenue process should include individuals from the sales department (deal directly with the customers), the legal department (draft or review contracts and sales agreements), the order entry department (process the orders), the accounting department (invoice the customer and record the revenue), the shipping department (ship the goods to customers), and the accounts receivable department (approve the credit limits and then collect the receivables). Based on the assessed risks, a response is developed that may include preventive controls (reducing the opportunity to commit fraud) or mitigation controls (reducing the impact of the potential fraud).

significant locations, significant accounts, relevant assertions, significant processes, and significant application systems, you were laying the groundwork for the risk assessment process.

Despite its seeming complexity, risk assessment is a fairly straightforward process that can be broken into three steps: (1) establish objectives, (2) identify risks, and (3) document the risk assessment process.

Establish Objectives

Setting objectives, according to the COSO framework, "is a precondition to risk assessment." That's because, quite simply, you have to set objectives before you can identify the risks that might hinder you from attaining those objectives.

Broadly, objectives fall into one of several categories, as follows:

- *operations objectives,* which address high-level issues such as profitability
- *compliance objectives*, which relate to conformance with applicable laws and regulations

But for the purposes of section 404 and this document, we are focusing primarily on:

- *financial reporting objectives,* which concern the accurate, complete, and timely preparation of financial reports

Objectives can be categorized as either "entity-level," which encompass the entire organization, or "process-level," which concern smaller scale actions and procedures.

Entity-Level Objectives

To begin the process of establishing entity-level objectives, COSO suggests that you start with broad statements that describe what you'd like the entire organization to achieve. Although objectives can address a wide variety of issues, such as market share (e.g., become the No. 2 manufacturer of aglets by the year 2005), revenue growth, or workforce expansion, for the purpose of section 404, the focus can be much narrower and simpler. Sample language for the primary entity-level objectives is provided below:

Publish reliable financial statements in accordance with generally accepted accounting principles that include those policies and procedures that:

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

Of course, the above-listed objectives are too generic and too broad for use in your section 404 project. You should more clearly define them for your particular circumstances, addressing each COSO component.

Your organization should also develop other entity-level objectives for the control environment, information and communication, and monitoring. Here are some samples for each:

Sample Control Environment Objectives
- management demonstrates character, integrity, and ethical values
- the company is committed to competence
- the audit committee and/or the board of directors are actively involved and have significant influence over the company's internal control over financial reporting

Sample Information and Communication Objectives
- financial reporting and related application and information systems are reliable
- appropriate and necessary information is obtained from, and provided to, management
- information is gathered from and disseminated to the appropriate people on a timely basis

Sample Monitoring Objectives
- internal audit's scope, responsibilities, and audit plans are appropriate for the company
- internal audit adheres to professional standards, such as those issued by The Institute of Internal Auditors
- the entity is responsive to internal and external recommendations

See Appendices C, D, and E for further details on these objectives.

Process-Level Control Objectives
After developing your broadly worded entity-level objectives, you should incorporate more detail in your process-level objectives. While your entity-level objectives will likely be relatively few, your process-level objectives may number in the hundreds.

Process-level objectives should be created for all the significant accounts and disclosures that you identified earlier. To accomplish this, use the financial statement assertions that you developed for significant accounts and disclosures.

For example, assume that the significant account you are setting objectives for is "sales." Because management should ensure that all revenue is recognized in the appropriate period, one possible financial assertion would be "completeness." (Other financial assertions may apply as well.) Once the financial assertion has been identified, relevant control objectives should be established. Under this example, one control objective for the sales account, derived from the financial assertion of completeness, may be the following: "All orders received from customers are input and processed."

Identify Risks

Entity-Level Risks
Entity-level risk affects what the overall entity — i.e., your entire company — wants to achieve. These risks typically impact "big picture" concerns.

Entity-level risks should be developed for each of the five components of COSO. Be especially sure to address the areas of control environment, information and communication, and monitoring, which are often overlooked in favor of the other COSO components. Begin with a "what-if?" process to consider each of your entity-level control objectives in each COSO area, and then create a detailed listing of risks to attaining those objectives. You can start by simply inverting the control objectives. For example, in the control environment area, if your objective is "the company is committed to competence," an associated risk may be that "the company is *not* committed to competence." However, that should be considered only a starting point, not an end point. You should then ask yourself: "What are the underlying risk factors that could hinder my company's commitment to competence?" You may find answers to that question in the areas of leadership, job descriptions, communication, hiring practices, performance reviews, and more. Each of these risk areas should be documented.

Process-Level Risks
Once your objectives are documented, you should identify any internal and external factors — risks — that may thwart or hinder your company from attaining its financial reporting control objectives.

As described previously, you can approach this process by creating "what if?" scenarios. Take each control objective and then try to envision what could go wrong. What are the situations, circumstances, and problems that could arise that might thwart your objectives?

Document the Risk Assessment Process

As with most facets of your section 404 project, full documentation is critical. Risk assessment is one of the five components of COSO that will require documentation to support compliance. Additionally, you will need documentation to support your internal control report, as well as for your independent auditors to perform testing and validation.

3.7 Controls in Action (Part I)

When companies strive to implement or strengthen their system of internal control, most tend to take a predictable course: They focus on the controls that address systematically processed transactions that flow through major general ledger accounts; they concern themselves with obvious business processes.

Yet, in our experience, far more errors occur elsewhere, in less familiar terrain. Some mistake-prone areas include application of accounting policies, non-routine events and transactions, information technology, and fraud.

Starting here and continuing in the next two sections (*Evaluate the Design of Controls* and *Test the Operating Effectiveness of Controls*), we will provide illustrative examples of these oft-overlooked controls and their associated objectives and risks.

The chart in Figure 2 is populated with sample data that lays out the critical information in a hypothetical situation. Listed atop the four columns are the categories of controls that often prove troublesome. Subsequent rows contain information similar to that which you will have gathered earlier in this document:

- sample business processes and significant accounts identified during scoping activities
- financial assertion associated with the business processes and significant accounts
- illustrative control objective for each category of control
- the risk associated with the control objective

Consider, for example, controls over authorization of non-routine events and transactions. Moving down the column, we find that a business process related to non-routine events and transactions involve financial closing and reporting, and that the accounts that are impacted by this activity are pervasive.

In the row labeled "illustrative objective," a sample objective for each category of control is provided. For example, in the "fraud" column, one possible objective is that "Recorded revenue represents valid transactions." Note that the objective provided in each category is simply one illustrative example. In actuality, you will have many — perhaps dozens — of objectives for each control category.

The next row addresses "risk." For each objective listed directly above it, a hypothetical risk has been assigned. As before, although only a single risk is listed here, any number of risks may actually exist for each objective.

Figure 2: Controls in Action - Part I

	Accounting Policies	Non-Routine Events and Transactions	Information Technology	Fraud
Business Process	Financial Closing and Reporting	Financial Closing and Reporting	Information Systems Management	Revenue
Account	All	All	N/A	Accounts Receivable, Sales
Financial Assertion	Existence or occurrence, completeness, valuation or allocation, rights and obligations, and presentation and disclosure	Existence or occurrence and presentation and disclosure	N/A	Existence or occurrence and rights and obligations
Illustrative Objective	The company's accounting policies reflect the most recent and applicable authoritative guidance and are properly documented, communicated, and applied consistently to events and transactions across business units and accounting periods.	Non-routine events and transactions are valid and properly recorded in the appropriate accounting period.	Logical security tools and techniques are implemented and configured to enable restriction of access to programs, data, and other information resources.	Recorded revenue represents valid transactions
Risk	The company does not properly apply authoritative literature (e.g., generally accepted accounting principles) to its financial transactions.	Significant non-routine events and transactions are not reviewed by individuals with the requisite technical expertise and are improperly recorded by the company.	Unauthorized individuals can access the company's financial accounting systems and make changes to the underlying financial data.	Revenue is recorded without having a properly completed sales transaction.

Note: The examples above are intended to be illustrative, not comprehensive. In practice you will have significantly more business processes, accounts, financial assertions, control objectives, risks, and control activities. Additionally, procedures to evaluate and test the design and operating effectiveness of control activities will be more comprehensive and require extensive documentation including reports reviewed, individuals interviewed, number and details of transactions selected, and more.

3.8 Evaluate the Design of Controls

Once control objectives are summarized and risks that may hinder those objectives are identified, astute managers might reasonably ask: "What can we do to minimize these risks?"

That's where control activities come in. Control activities are policies and procedures that help your company mitigate risk and meet its objectives. In the case of section 404, control activities will help you attain your entity-level objective of producing timely and reliable financial reports, and your multiple process-level objectives designed to effect the same.

Control activities can be seen as part of a continuum: First you developed your objectives; next you identified risks for each objective; now you associate control activities with each risk.

Getting a Handle on Control Activities

In the broadest sense, controls can be divided into two main categories: company-level controls and process-level controls.

Company-level controls typically exist and operate across an organization (both single location and multiple location companies). These controls are designed to monitor the appropriateness and reasonableness of the information provided by the underlying processes (and locations), and to monitor the effectiveness of the controls that operate within a process (and across multiple locations). Examples of company-level controls include corporate-level controls over common processes and systems, centralized financial processing, and consistent period-end financial reporting procedures and processes.

Process-level control activities generally operate at a number of levels:

- At senior levels of management, the control activities are more likely to be high-level procedures performed by management and are likely to involve greater aggregation of data and less consideration of detail.
- At lower levels, the control activities are likely to be focused on distinct sets of data and at a much greater level of detail.
- At the lowest level, detailed control activities are likely to relate to specific transactions.

Major control types include preventive, detective, manual, and information technology. Here's a primer:

Preventive: Preventive controls are designed to avert problems rather than identify them. Some examples include the use of passwords to gain access to computer application systems, or required approval for all purchase orders over a certain dollar threshold.

Detective: Detective controls are meant to identify errors or irregularities after the fact. These may take the form of reviews, reconciliations, and analyses.

Manual: Manual controls are carried out by people, as opposed to automated controls (i.e., application controls) that take place without direct human intervention. An employee manually reconciling a bank statement or a manager reviewing sales based on budgeted amounts are examples of manual controls.

Information Technology: Information technology (IT) controls are controls over computer processing of information, consisting of general controls (including controls over data center operations, system software acquisition and maintenance, access security, and application system development and maintenance) and application controls (designed to ensure completeness, accuracy, authorization, and validity of data input and transaction processing).

Examples of commonly performed control activities include the following:

Reviews: Reviews are usually one of three types: analytical (evaluating summary information by comparing it with expected results), transactional (checking the accuracy of output by comparing it, in detail, with expected results), or performance (examining documentation to determine that control activities were performed as intended). Each type can be found in both IT systems and manual processes. However, all reviews typically include some manual elements. For example, management may conduct a manual review in follow-up to an IT-generated report of large or unusual transactions. To be effective, reviews should be performed by personnel who have the knowledge and experience to identify relevant exceptions and errors.

Reconciliations and Comparisons: Recorded assets should be reconciled and compared with independent records. Reconciling a bank statement to its associated general ledger account is one example of this type of control activity.

Safeguarding of Assets: To ensure the integrity of your financial reporting, you should safeguard your company's assets against misappropriation, errors, and irregularities. In its auditing standard, the PCAOB provided a definition that companies should refer to when identifying controls over safeguarding of assets:

Safeguarding of assets are those policies and procedures that "provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the company's assets that could have a material effect on the financial statements."[17]

Interestingly, your company could sustain a loss of assets through misappropriation and still be deemed to have effective internal control — if the loss is detected and properly represented in the financial statements. According to COSO, "to the extent that such losses might occur, controls over financial reporting are effective if they provide reasonable assurance that those losses are properly reflected in the financial statements, thereby alerting financial statement users to consider the need for action."[18]

That element of the rule notwithstanding, we recommend instituting sufficient preventive controls to properly safeguard company assets.

Information Technology Controls: In many companies, the use of computers is pervasive, the computer processing environments are complex, and the application systems are vital to the business. In such instances, it is likely that the effectiveness of control activities (manual and application) are dependent on whether the computer processing environment supports the reliable processing of financial information.

[17] "Release No. 2004-001: Auditing Standard No. 2, An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements," Public Company Accounting Oversight Board, 2004. Electronic copy can be viewed at: http://www.pcaobus.org/rules/Release-20040308-1g.pdf.

[18] Committee of Sponsoring Organizations (COSO) of the Treadway Commission's Addendum, Reporting to External Parties, 1994.

The Complex World of Information Technology Controls

The requirements and procedures for establishing internal control over information systems are technical and extensive. For detailed guidance, see *IT Control Objectives for Sarbanes-Oxley: The Importance of IT in the Design, Implementation, and Sustainability of Internal Control Over Disclosure and Financial Reporting,* a recent publication from The Information Systems Audit and Control Association. This publication, which draws upon the CobiT[19] framework, provides specific control objectives and control activities that may be considered when designing information technology controls based on the COSO internal control framework. For a copy, visit http://www.isaca.org.

Information technology controls can be broken down into two types:

1. *General Controls:* According to COSO, general controls, which are designed to ensure that the financial information that is generated from a company's application systems can be relied upon, include the following types of controls:
   - Data center operation controls — controls such as job set-up and scheduling, operator actions, backup and recovery procedures, overall systems availability, and contingency or disaster recovery planning.
   - System software controls — controls over the effective acquisition, implementation, and maintenance of system software, database management, telecommunications software, security software and utilities.
   - Access security controls — controls that prevent inappropriate and unauthorized use of the system.
   - Application system development and maintenance controls — controls over development methodology, which includes system design and implementation, outlining specific phases, documentation requirements, approvals, and checkpoints to control the development or maintenance of the project and version control.
2. *Application Controls:* Application controls are embedded within software programs to prevent or detect unauthorized transactions and allow the authorization and processing of transactions. When combined with manual controls, as necessary, application controls ensure the completeness, accuracy, authorization, and validity of processing transactions.

   Some examples of application controls include:
   - Balancing control activities — These controls detect data entry errors by reconciling amounts captured either manually or automatically to a control total. For example, a company automatically balances the total number of transactions processed and passed from its online order entry system to the number of transactions received in its billing system.
   - Check digits — These controls use calculations to validate data. For example, a company's part numbers may contain a check digit to detect and correct inaccurate ordering from its suppliers. Universal Product Codes include a check digit to verify the product and the vendor.
   - Predefined data listings — These controls provide the user with predefined lists of acceptable data. For example, a company's Intranet site might include drop-down lists of products available for purchase.
   - Data reasonableness tests — These controls compare data captured to a present or learned pattern of reasonableness. For example, an order to a supplier by a home renovation retail store for an unusually large number of board feet of lumber may trigger a review.
   - Logic tests — These controls include the use of ranges limits or value or alphanumeric tests. For example, a government agency detects potential errors in social security numbers by checking that all entered numbers are nine digits in length.
   - Authorization controls — These controls establish accountability for the initiation and approving of transactions that impact the financial reporting process.
   - Tolerance levels — These controls specify who can initiate or authorize certain transactions over dollar limits without approval. Similar provisions may be made for journal entries.

Which Controls Should Be Evaluated?

Basically, you need to evaluate the controls that meet the control objectives for each of the relevant assertions for the significant accounts and disclosures that you previously identified. But it's not entirely up to your discretion. In its rulemaking, the SEC has identified certain controls as significant by default. Any controls that fall under these categories should be evaluated:

- controls related to the initiation, recording, processing and reconciling of account balances, classes of transactions, disclosures, and related assertions included in the financial statements
- controls related to the initiation and processing of non-routine and non-systematic transactions
- controls related to the selection and application of accounting policies
- controls related to the prevention, identification, and detection of fraud[20]

In addition to the controls listed above, the PCAOB has identified in its auditing standard additional controls that warrant attention.

- controls, including information technology general controls, on which other controls are dependent. General controls include:
  - data center operation controls
  - system software controls
  - access security controls
  - application system development and maintenance controls
- controls over significant non-routine and nonsystematic transactions, such as accounts involving judgments and estimates
- company-level controls, including the control environment and controls over the period-end financial reporting process, including controls over procedures used to enter transaction totals into the general ledger; to initiate, authorize, record, and process journal entries in the general ledger; and to record recurring and nonrecurring adjustments to the financial statements (for example, consolidating adjustments, report combinations, and reclassifications)[21]

[19] "Control Objectives for Information and Related Technology," IT Governance Institute, 2000. Electronic download available here: www.isaca.org/cobit.htm.
[20] "Final Rule: Management's Reports on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports," U.S. Securities and Exchange Commission, 2003. Electronic copy can be viewed at: http://www.sec.gov/rules/final/33-8238.htm.
[21] "Release No. 2004-001: Auditing Standard No. 2, An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements," Public Company Accounting Oversight Board, 2004. Electronic copy can be viewed at: http://www.pcaobus.org/rules/Release-20040308-1g.pdf.

Map Control Activities to Control Objectives

Every control objective that you identified earlier should have one or more corresponding control activities. To ensure that you have not overlooked any objectives or controls, perform a systematic analysis. Examine your master list of control objectives and map the corresponding control activities against them.

For example, if one of your control objectives is, "Invoices are recorded in the appropriate period," you should determine if you have a control activity in place to meet that objective. One such control activity might be, "Goods shipped at, before, or after the end of an accounting period are examined and reconciled to ensure complete and consistent recording in the appropriate accounting period, including the raising and recording of the related invoices."

Evaluate Design Effectiveness

With your control activities neatly mapped to your objectives, you should now assess the design effectiveness of your controls. Basically, you (and, soon, your independent auditors) will be seeking evidence that your controls are properly constructed to achieve the related control objectives. In compiling this evidence, make note of the following:

- *owner of control:* identification of person(s) responsible for executing the control
- *description of process flow:* detailed explanation of how the control operates
- *properly designed?* Is the control built correctly? In other words, if the control is used as directed, will it accomplish the objective?
- *details of the internal control deficiency:* If the control is deemed deficient, what are its specific shortcomings?
- *remediation plan:* How will the faulty design be corrected?

The specific methods you use to evaluate the design of controls will depend on several factors:

- the types of control activities you are evaluating, including whether manual or programmed
- competence of the individuals who perform the relevant control activities
- the period of intended reliance
- the use of a service organization
- regulatory and governmental requirements

Classify Design Deficiencies

If the efforts outlined above reveal that the design of certain control activities is less than optimal, then you'll need to determine the level of severity of the failure. The internal control design deficiencies will fall into one of three categories: (1) material weaknesses, (2) significant deficiencies, or (3) internal control deficiencies considered to be insignificant or deficiencies for which mitigating controls exist. In general, if the design of the control is insufficient to achieve its related control objective, then this should be considered at least a significant deficiency. (For more information on the classification of material weaknesses and significant deficiencies, see Appendix B.)

Don't Miss Missing Controls

Once the above-listed processes are complete, you will likely have identified control objectives for which no corresponding control activities exist. Document these missing controls and remediate as outlined in the following section.

Develop and Implement Remediation Plan

Your final task in the control design phase is to fix the internal control deficiencies that you have uncovered. This may involve strengthening controls that have "fixable" design weaknesses; overhauling controls with more significant problems; discarding old and implementing new controls when the internal

Internal Control - A Taxing Problem?

In our discussions with hundreds of tax professionals, we've learned that relatively few tax departments have had well-documented controls, and independent auditors have seldom placed heavy reliance on any controls they found. Instead, independent auditors have typically conducted extended substantive testing to evaluate complex tax computations and analyses. Consequently, unlike other departments, tax departments have seldom been put through the rigors of an internal control review. That, of course, has all changed as a result of Sarbanes-Oxley.

Tax-specific controls are crucial because:

- Tax can represent one of the largest line-item expenses on a company's income statement; and taxes paid, tax assets and liabilities, and tax-related disclosures represent material, integral components of a company's statement of cash flows, balance sheet, and footnotes.
- Pressure to meet earnings goals and present steady effective tax rates may tempt individuals within a company to implement overly-aggressive tax planning strategies or underestimate the appropriate reserves for its tax contingencies.
- The proper identification and classification of tax assets and liabilities can affect whether a company's ratios satisfy its debt covenants.
- Stories of corporate tax avoidance, tax shelters, and sham transactions continue to appear in the media, and audit committees are demanding a much higher level of understanding of the process each company takes when determining its tax-planning activities.
- In many companies, the likelihood of spotting tax errors outside the tax department is very low, so the importance of tax controls is even more critical to help protect the integrity of the financial statements.

The fundamental steps for ensuring tax function readiness are no different than those for any other internal control process. They include:

- identifying financial reporting and disclosure risks related to significant tax processes (management, reporting, and planning) and tax types (including multi-state, international, and employee benefits taxes), regardless of whether those taxes are included under the tax department's jurisdiction
- identifying relevant control activities
- documenting, evaluating, and testing the design and operating effectiveness of significant tax controls

Figure 3: Controls in Action - Part II

	Accounting Policies	Non-Routine Events and Transactions	Information Technology	Fraud
Control Activity	Accounting policies and procedures, standard charts of accounts, and related guidance are updated annually.	Information about all significant non-routine events and transactions is documented for analysis in a timely manner. Management reviews all significant non-routine events and transactions prior to recording.	The identity of users (both local and remote) is authenticated to the system through passwords or other authentication mechanisms. The policies relating to use of passwords require periodic password change, confidentiality requirements and password format (e.g., password length, alphanumeric content).	The completeness of key terms in the underlying sales contract is confirmed with the signatory of the contract.
Owner of Control	Corporate Controller	CFO	IT Manager	Sales Manager
Properly Designed?	No	Yes	Yes	Yes
Details of Design Deficiency	Accounting policies and procedures, standard charts of accounts, and related guidance are not updated frequently enough. In addition, such items are not distributed to subsidiaries.	N/A	N/A	N/A
Remediation Plan	Update quarterly accounting policies and procedures, standard charts of accounts, and related guidance and distribute to subsidiaries.	N/A	N/A	N/A

Note: The examples above are intended to be illustrative, not comprehensive. In practice you will have significantly more business processes, accounts, financial assertions, control objectives, risks, and control activities. Additionally, procedures to evaluate and test the design and operating effectiveness of control activities will be more comprehensive and require extensive documentation including reports reviewed, individuals interviewed, number and details of transactions selected, and more.

control design deficiency is too substantial to be repaired through tinkering; and instituting new controls wherever they have been found to be entirely missing.

3.9 Controls in Action (Part II)

The chart that we introduced in section 3.7 (Figure 2) has now been expanded to include control activities as shown in Figure 3. That is, for each control objective listed in the chart, a control activity has been assigned to accomplish that objective. New entries also include the following: *owner of control* (identification of person(s) responsible for executing the control); *properly designed?* (is the control built correctly?); *details of design deficiency* (if not, what are the problems with the control?); and *remediation plan* (how will the faulty design be corrected?). (Note that the chart is torn off at the top; only new entries are included here.)

3.10 Test the Operating Effectiveness of Controls

All of the work you have performed up to this point leads to the task that many people consider the crux of section 404: testing the operating effectiveness of control activities.

Control Limits

Even the best-designed and best-operating controls are not fail-safe. A number of factors can weaken or circumvent internal control, including the following:

- Breakdowns: Even if controls are well-designed, they can break down due to carelessness, distraction, or fatigue. For example, an accounting department supervisor responsible for investigating exceptions might simply forget or fail to pursue the investigation far enough to be able to make appropriate corrections. Temporary personnel executing control duties for vacationing or sick employees might not perform them correctly.
- Management override: A system of internal control can only be as effective as the people who are responsible for its functioning. Even in effectively controlled entities — those with high levels of integrity and control consciousness — a manager might have the ability to override certain control activities.
- Collusion: Individuals acting collectively to perpetuate and conceal an action from detection often can alter financial data or other management information in a manner that cannot be identified by the control system. For example, there may be collusion between an employee performing an important control function and a customer, supplier, or another employee. On a different level, several layers of sales or divisional management might collude in circumventing controls so that reported results meet budget or incentive targets.

Plan Tests of Controls

Who should perform these tests? Any number of people may do so, including internal audit, company management, certain outside consultants under the direction of company management or the audit committee, and even the employees responsible for enacting the controls. However, by regulation, your independent auditors are prohibited from performing these tests on behalf of management. That's because at the end of the process, your independent auditors issue their report on the effectiveness of your internal control over financial reporting and whether management's assessment of the effectiveness of internal control over financial reporting is fairly stated. If your independent auditors conducted the tests and then opined on the effectiveness of those tests, they would, essentially, be testing their own work.

What are these tests supposed to accomplish? A couple of things: For one, the tests are designed to ensure that control activities are functioning properly. For another, the tests will support that vital section 404 report — *Management's Report on Internal Control Over Financial Reporting.*

Your independent auditors are permitted to rely to a certain extent on your testing activities. But your independent auditors will rely on this evidence only if they are assured of the competence (based on experience and training) and objectivity (based on independence from management and lack of day-to-day responsibility for the control activity) of your people who perform the work. The higher the objectivity and competence levels, the more your independent auditors may use your work.

If your company deploys a self-assessment process (a description of self-assessment is provided in section 3.14, *Monitor the System of Internal Control*), which is a practical method of obtaining timely evidence, particularly in large, multiple-location entities, the amount of testing you conduct will depend on your organizational structure. One approach might be that each person responsible for performing a control also is responsible for self-assessing the performance of the control. In that case, the person would likely have firsthand knowledge as to whether the control was operating. Your independent auditors will not be able to rely on your self-assessment testing when conducting their evaluation and testing procedures, yet the existence of a comprehensive self-assessment process may provide evidence of a strong system of internal control.

Certain testing activities, most notably those involving the control environment, must be conducted solely by the independent auditors without any reliance on testing by other parties.

As you plan your tests of controls, keep these points in mind:

- Inquiry alone is not adequate; extensive testing procedures should be carried out. For example, telephoning the payroll clerk and asking if employee timesheets are reconciled with accrued vacation time is insufficient. The actual written records should be reviewed and the action documented.
- Management should not rely solely on self-assessment procedures. Although employees can be deployed to test controls under a self-assessment process, there should be some independent monitoring of their procedures. That is, the person who performs the control cannot simply verify that the control is operating effectively. There should be some independent evaluation. (This will be discussed in further detail in section 3.14, *Monitor the System of Internal Control.*)
- If your company uses an outside service provider for certain business functions, you should request from the provider a SAS 70 report, which reports on the effectiveness of internal control at the outside company. Note that this should be a "Type 2" report. (Type 1 reports only address the design of the controls, while Type 2 covers both the operating effectiveness and design.) (To identify service organizations for which this requirement applies, see *Identify Service Organizations and Other Extended Relationships,* in section 3.5.)

Perform Tests of Controls

Which controls should be tested for operating effectiveness? Simple: the same controls that you selected earlier for evaluating design effectiveness.

Tests of controls are usually performed using the following techniques, often in combination:

Corroborative Inquiry: This procedure, consisting of detailed interviews to obtain evidence about the effectiveness of controls, is performed in tandem with other procedures (e.g., examination of documentary evidence) to corroborate the information derived from the inquiry.

The detailed interviews may include direct and/or indirect inquiries:

- Direct inquiry involves asking questions of the individual who performs the control activity being tested.

- Indirect inquiry involves asking questions of other individuals who do not perform the control activity themselves but are in a position to know whether the control activity is operating effectively.

Observation: Observing the performance of a control activity often provides substantial evidence of its effectiveness. For example, you may test controls over inventory by observing that employees who perform and record the counts follow management's written instructions.

But observation of a control activity in action ordinarily does not, in itself, provide sufficient evidence of the effectiveness of the control activity, mainly because observations may not be representative of the usual performance of a control activity because management and staff may perform their tasks more diligently if they know they are being observed. Consequently, you should perform supplementary procedures, such as inquiries or re-performance, to augment your results.

Examination of Documentation: If performance of a control activity is documented, you can obtain evidence of its performance by examining the documentation, both electronic and written. The level of assurance you can obtain from such evidence will depend on the nature of the control activity. For example, if the performance of the control activity is documented by the initials of the performer, examination of the initials provides little evidence of the effectiveness of the control activity. On the other hand, documentation of reconciliations, including follow-up and resolution of unusual items, may contain information that provides evidence of the effectiveness of the control activity.

Re-Performance: Although re-performance of a control activity sometimes provides evidence of its effectiveness, such evidence is rarely persuasive by itself because the mere absence of errors in the items tested does not provide conclusive evidence that the control activity has historically been performed effectively. This is particularly true of manual control activities.

Re-performance may be effective for testing application controls, because the computer processes transactions systematically. For example, a tester may attempt to enter flawed transactions into a computer application. If the computer application controls cause the faulty transactions to be rejected, you will have evidence that these controls are operating effectively. (Note that you should take precautions with these types of tests to ensure that the tests do not themselves cause misstatements!)

Remember, your testing *procedures* need to be as thoroughly documented as the test *results*. Otherwise your independent auditors will be forced to replicate your work rather than relying on it to the greatest extent possible.

Document Test Results

Your evaluation of control activities will likely yield a mixed bag of results — some controls will function as designed; others will not.

If the control is operating effectively, document the successful control test. Success is great, but insufficient. If you deem your controls effective, you should provide documentary evidence. (Remember that you are responsible for obtaining at least the same level of assurance as your independent auditors, so be sure to consult with them early in the process.)

Maintained in a database, spreadsheet, or your permanent files, and available for inspection by your independent auditors, regulatory personnel, and other authorized parties, should be complete descriptions of the following:

- tests performed and evidence obtained
- results of the tests
- conclusion as to the effectiveness of each control tested

If the control is not operating effectively, document the internal control deficiency. In virtually every organization, internal control deficiencies will be uncovered through the testing process. You should now determine the cause and significance of each internal control deficiency you've identified. Start by analyzing the particular circumstances and reasons for the deficiency. Document the details of the individual control deficiencies. Then aggregate and summarize all the deficiencies you've identified.

Classify Internal Control Deficiencies

Next, you should determine whether the internal control deficiency should be classified merely as an "internal control deficiency" or if it is more serious and represents a "significant deficiency" or a "material weakness." (For additional information on the characteristics of an internal control deficiency, significant deficiency, and material weakness, see Appendix B.)

To determine whether an internal control deficiency is a significant deficiency or a material weakness generally requires substantial analysis and judgment.

Pay Attention to Period-End Financial Reporting Processes

As you identify significant processes, take care to include those that support period-end financial reporting. According to the PCAOB, the period-end financial reporting process is *always* significant because of its importance both to financial reporting itself, as well as to the independent auditors' opinions on internal control over financial reporting and the financial statements.

The period-end financial reporting process includes (but may not be limited to) the following:

- procedures used to enter transaction totals into the general ledger
- procedures used to initiate, authorize, record, and process journal entries in the general ledger
- other procedures to record recurring and nonrecurring adjustments to the annual and quarterly financial statements, such as consolidating adjustments, report combinations, and classifications
- procedures for drafting annual and quarterly financial statements and related disclosures

Note that timing is critical here: Your company needs to document this process. You and your independent auditors will also need to evaluate and test the related control activities at least for one interim quarterly closing process and the annual year-end closing process.

Figure 4

Type of Deficiency	Likelihood of Occurrence		Magnitude of Misstatement
Internal control deficiency	Remote	and/or	Inconsequential
Significant deficiency	More than remote	and	More than inconsequential
Material weakness	More than remote	and	Material

Further complicating the issue, internal control deficiencies cannot just be considered in isolation; their potential impact on the financial statements should also be considered in the aggregate.

Fundamentally, classification of an internal control deficiency is predicated on the:

- likelihood that an internal control deficiency, or a combination of internal control deficiencies, could result in a misstatement of an account balance or disclosure
- magnitude of the potential misstatement resulting from the internal control deficiency or internal control deficiencies

To assist in classifying internal control deficiencies, use the table shown in Figure 4.

Using the table, first determine whether the likelihood that the internal control deficiency could result in a misstatement of an account balance or disclosure is remote or more than remote. (The Financial Accounting Standards Board defines remote as "the chance of the future event or events occurring is slight.")[22] Next, calculate the magnitude of the misstatement that could result in the financial statements because of this internal control deficiency. For example, if the deferred tax calculation was prepared by an individual that lacks knowledge of tax-related accounting matters and if it was not appropriately reviewed and approved by someone who is more experienced than the preparer and has the relevant tax-related knowledge, determine what the possible misstatement could be. In many circumstances, this error could be material and the lack of a control could thus be determined to be a material weakness.

When prioritizing which internal control deficiencies to remediate first, start with material weaknesses, work through significant deficiencies, and finish with the remaining internal control deficiencies where the benefit exceeds the cost and risk of not remediating.

Develop Remediation Plan

Once the internal control deficiencies have been categorized and prioritized, you are ready to develop your internal control remediation plan. As you design the specific internal control remediation process or solution, make sure that the necessary internal control objectives are met and that identified risks are addressed. You should designate a process owner or champion for each plan, develop a remediation timeframe, and provide detailed cost estimates and estimated work effort.

If your plan includes the remediation of material weaknesses and significant deficiencies, ensure that your remediation efforts commence immediately. Otherwise you may not have sufficient time to ensure that the remediated control activity is operating effectively prior to your first internal control audit. And, as you probably now know, a material weakness would preclude your independent auditors from issuing an unqualified opinion on the effectiveness of your internal control over financial reporting.

Implement Remediation Plan

Before putting your remediation plan into action, you'll want to get the proverbial "buy-in" from all the various parties who will be involved in and affected by the project. Be especially diligent about communicating the plan to your independent auditors, top executives, and the audit committee.

As a means of staying on track, it will be important to identify steps and key milestones in achieving resolution within the required timeframes. You'll want to monitor your progress against established milestones, and report progress and issues to the internal control steering committee.

You'll need to perform additional testing once control activities have been updated to be sure that remediation is complete and controls are operating effectively. Check to ensure that documentation has been updated to reflect each resolved internal control deficiency and new control activities.

3.11 Controls in Action (Part III)

The final version of our expanding chart (Figure 5) includes several new rows. The new entries include the following: *test of control* (what steps will be taken to test the control?); *operating effectively?* (does the control work as designed?); *details of operating deficiency* (detailed description of operation flaws); *remediation plan* (how will the faulty control be fixed?). (Note that the chart is torn off at the top; only new entries are included here.)

[22] "FAS 5: Accounting for Contingencies," Financial Accounting Standards Board, 1975.

Figure 5: Controls in Action - Part 3

	Accounting Policies	Non-Routine Events and Transactions	Information Technology	Fraud
Test of Control	Because the control was not designed effectively, it cannot operate effectively.	Member of the project team interviewed the individual that prepared the analysis of significant non-routine events and transactions to understand the steps involved in preparing the report. Member of the project team tested a sample of significant non-routine events and transactions by reviewing documentation that supports the CFO's review. In addition, member of the project team interviewed the CFO to understand the nature of his/her review and steps that were taken to address transactions, which do not appear to be valid.	Member of the project team observed that the system is configured to force user authentication in accordance with company policies, the system does not allow blank or simplistic passwords and that the application encrypts passwords when entered into the system. In addition, member of the project team attempted to gain unauthorized access to the system by using different combinations of user IDs and passwords.	Member of the project team understood and documented the policies and procedures related to the confirmation of key terms in the sales contract. Member of the project team interviewed individuals who prepare the confirmations to understand the steps involved in preparing and mailing the confirmations, the reports or other information used, any exceptions or unusual items noted, disposition of exceptions identified, and any instances where the control activity operated in a way contrary to their understanding of how it should operate. Member of the project team tested a sample of contracts to ensure that the selections made by the company were in accordance with their policies and procedures. In addition, member of the project team reviewed a selection of responses received from the signatory to ensure appropriate treatment.
Operating Effectively?	No	No	Yes	Yes
Details of Operating Deficiency	Because the control was not designed effectively, it cannot operate effectively.	The CFO did not review three of the journal entries selected for review.	N/A	N/A
Remediation Plan	Corrected design deficiencies; tested operating effectiveness in the next period.	Emphasized to the CFO the need to review all journal entries related to estimates; test operating effectiveness in the next period.	N/A	N/A

Note: The examples above are intended to be illustrative, not comprehensive. In practice you will have significantly more business processes, accounts, financial assertions, control objectives, risks, and control activities. Additionally, procedures to evaluate and test the design and operating effectiveness of control activities will be more comprehensive and require extensive documentation including reports reviewed, individuals interviewed, number and details of transactions selected, and more.

Figure 6

Objective	Sample Activity
Integrity and ethical values	Management maintains a code of conduct and other policies regarding acceptable business practices, conflicts of interest, and expected standards of ethical behavior.
Commitment to competence	Formal job descriptions are in place that consider the degree to which individuals must exercise judgment and are subject to supervision.
Board of directors / audit committee	A process exists for the audit committee to be informed promptly and anonymously, when appropriate, of significant issues.
Management's philosophy and operating style	Management adopts accounting policies that best reflect the economic realities of the business.
Organizational structure	Management periodically evaluates the entity's organizational structure and makes changes as necessary based upon changes in the business or industry.
Assignment of authority and responsibility	Management determines and clearly communicates the responsibilities and expectations of the finance and accounting departments.
Human resource policies and procedures	Management establishes and enforces standards for hiring the most qualified individuals, with emphasis on educational background, prior work experience, past accomplishments, and evidence of integrity and ethical behavior.

3.12 Create an Effective Control Environment

The control environment represents a unique component of your system of internal control. Composed of hard-to-measure elements such as tone at the top, ethical values, integrity, philosophy, and operating style, the control environment demands a unique approach to evaluating, testing, remediating, and monitoring.

Evaluate the Design Effectiveness of the Control Environment

To establish an effective control environment, each of the control environment objectives you developed earlier (section 3.6, E*stablish Objectives and Identify Risks*) should be associated with properly designed activities. Start by identifying and documenting activities currently in place that support the achievement of the control environment objectives.

Sample activities for various control environment objectives are included in Figure 6. (See Appendix C for an expanded list of objectives and activities.)

Test the Operating Effectiveness of the Control Environment

How shipshape is your control environment? You won't know until you test it!

The unique characteristics of the control environment call for testing activities that can differ markedly from those of other components of internal control. Several testing approaches are possible, including the following:

Interviews: Identify employees to interview at corporate and business units of the company. This list should include individuals from management, operations, finance, ethics and compliance, internal audit, and HR management. Focus your interviews on assessing the control activities that address the control objectives within the control environment.

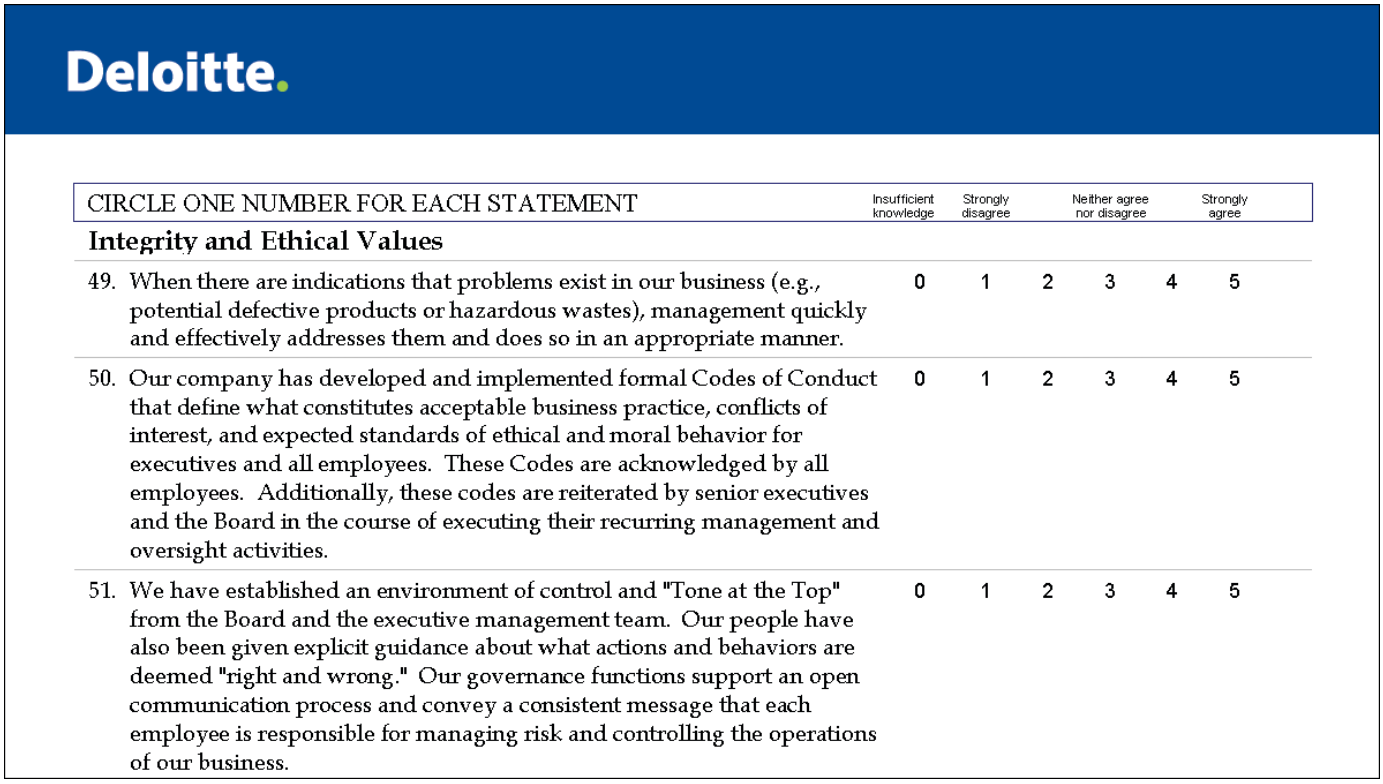
Cultural Assessment: The operating effectiveness of many of the control environment activities can be ascertained relatively quickly through a cultural assessment, which is a comprehensive analysis of the elements that make up the control environment. Your objectives should be:

- to test the operating effectiveness of the activities supporting the control environment objectives
- to understand whether your corporate compliance and ethics program is effective

Some planning work is required prior to conducting the assessment. You should:

- define the use of surveys and self-assessments
- integrate the use of the survey into the everyday responsibilities of the individuals who are asked to complete it
- set parameters for ongoing and final documentation
- identify document reviewers
- determine a process for handling the results of the assessment
- identify control environments to assess

Figure 7



Deloitte.

CIRCLE ONE NUMBER FOR EACH STATEMENT	Insufficient knowledge	Strongly disagree		Neither agree nor disagree		Strongly agree
Integrity and Ethical Values						
49. When there are indications that problems exist in our business (e.g., potential defective products or hazardous wastes), management quickly and effectively addresses them and does so in an appropriate manner.	0	1	2	3	4	5
50. Our company has developed and implemented formal Codes of Conduct that define what constitutes acceptable business practice, conflicts of interest, and expected standards of ethical and moral behavior for executives and all employees. These Codes are acknowledged by all employees. Additionally, these codes are reiterated by senior executives and the Board in the course of executing their recurring management and oversight activities.	0	1	2	3	4	5
51. We have established an environment of control and "Tone at the Top" from the Board and the executive management team. Our people have also been given explicit guidance about what actions and behaviors are deemed "right and wrong." Our governance functions support an open communication process and convey a consistent message that each employee is responsible for managing risk and controlling the operations of our business.	0	1	2	3	4	5

Regarding the final bullet, your company may have multiple control environments that should be assessed, including extended geographies (especially for multinational organizations) and business units.

Sample Control Environment Survey: In Figure 7 there are sample questions from a survey that Deloitte provides to its clients to help them evaluate the design and test the operating effectiveness of their control environment.

Regardless of your methodology, your control environment assessment should measure the following:

- employee awareness and perceived effectiveness of the company's system of internal control
- success at fostering an ethical culture and developing a sustainable control environment
- internal best practices for improving the control environment and ethical culture
- employee awareness and perceived effectiveness of the company's ethics and compliance program

The results of the interviews and surveys should be combined with other documentary evidence (e.g., reading of existing ethics and compliance policies and procedures). A summary of the assessment, along with preliminary conclusions and expected remediation actions, should be documented. To facilitate this process, consider using the *Control Environment Assessment Template* found in Appendix C.

Remediate the Control Environment

Once you have evaluated the design and tested the operating effectiveness of your control environment, you should set about correcting any problems that you've uncovered.

Prioritize Identified Deficiencies

Moving through each identified internal control deficiency, determine whether it is a design deficiency or an operating deficiency.

For example, an employee's failure to abide by the company code of ethics may be attributable to various factors, such as:

- the code is not distributed to all employees (design deficiency)
- the employee neglected to read the existing code of ethics (operating deficiency)
- the employee did not use components of the ethics program (such as the whistleblower hotline) because the employee feared retaliation (operating deficiency)

Once you have categorized internal control deficiencies in this manner, you should prioritize the deficiencies based on the perceived level of risk to the company. In most cases, that risk level will be high. The PCAOB has indicated that an ineffective control environment "should be regarded as at least a significant deficiency and as a strong indicator that a material weakness in internal control over financial reporting exists."[23]

Develop Remediation Plan

Depending on the flaws uncovered in the control environment, remediation may be manual (e.g., a policy, procedure, communication, monitoring, or cultural change) or system-related (e.g., system modification, reporting). For each internal

[23] "Release No. 2004-001: Auditing Standard No. 2, An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements," Public Company Accounting Oversight Board, 2004. Electronic copy can be viewed at: http://www.pcaobus.org/rules/Release-20040308-1g.pdf.

Wanted: Code of Ethics

A comprehensive code of ethics is considered obligatory when it comes to creating a strong control environment. As you develop your code, consider the following suggestions:

- Keep language simple and concise. Avoid jargon and legalese.
- Don't write in a "thou shalt not" format, but rather state expected behaviors.
- Apply the code evenly to all employees and board members across divisions and geographies. (Some companies take this a step further and apply their code to all stakeholders, including vendors and suppliers.)
- Convene a team that draws from a cross-section of departments, titles, and locations.
- Revise and update the code as needed to reflect business changes, regulatory changes, etc.
- Simply having a good code is not enough — you need to make sure people actually understand it, comply with it, and are not afraid to use it.

A code of ethics should include the following:

- an introductory letter from management that sets the tone at the top and defines the importance of ethics and compliance to each employee and the company
- the company's mission statement, vision, values, and/or guiding principles, which should reflect the company's commitment to ethics, integrity and quality
- guidance to assist employees in making the sound choices
- a listing of resources for obtaining guidance and for reporting of suspected misconduct:
  - anonymous reporting mechanism; employee help-line; whistleblower line
  - ethics and compliance officer/office
  - reporting chain of command (e.g., supervisor, department head)
  - ethics and compliance Intranet site
- enforcement and implementation mechanisms (e.g., unethical behavior will be subject to disciplinary action, which includes termination)
- examples of acceptable and unacceptable behavior

control deficiency noted, management should identify the following:

- business units and locations responsible
- priority (high, medium, low)
- responsible party
- remediation plan
- key milestones (including timeframe and estimated work effort)

Obtain Agreement From All Parties

Next you should ensure that members of the steering committee, executive management, finance function, ethics and compliance, internal audit, and communications are in agreement with all aspects of the remediation plan. Share the plan (and the assessment) with your independent auditors and the audit committee.

Implement Remediation Plan

Depending on the nature of the internal control deficiencies uncovered, remedial steps may include the following:

- Leadership: Set the "tone at the top"; ensure consistency of support, visibility, and message; reduce conflicting views at senior levels.
- Communications: Communicate the importance of internal control; reinforce the company's code of ethics; increase awareness; establish multiple channels for open, two-way communication, including anonymous reporting mechanisms.
- Training: Ensure employees understand the impact and importance of Sarbanes-Oxley and internal control; develop appropriate skills for compliance; educate employees on new policies or processes; conduct training and awareness programs.
- Organizational governance: Refine roles and responsibilities of the board of directors, leadership, and key business functions; ensure governance model maintains necessary controls.
- Metrics development: Work with the business to define measures of compliance and improvement.
- Personnel: Create new positions; modify existing roles and responsibilities; or remove existing personnel from their position, as required.
- Follow-up: Report to management and the audit committee the steps taken to correct the control deficiencies.

Clearly, a deficient control environment is not something that can be transformed overnight. Although the steps outlined in this section cover only a few pages, your activities may in fact span several months.

3.13 Communicate Information

In this age of razor-thin margins, hyper competition, and aggressive regulation, information and communication takes on heightened importance. The manner in which your company receives, analyzes, and disseminates information not only has a bottom-line impact, but also represents a key element of an effective system of internal control. According to COSO, *"… having the right information, on time, at the right place is essential to effecting control …"*.

Financial information serves external needs: Investors, analysts, and regulators judge you by it. Yet it also serves an important internal purpose: It tells you how the company is doing; helps you make decisions; and aids in budgeting, evaluating, and planning.

Information and Communication: A Primer

Information and communication, as it relates to internal control over financial reporting, is simply identifying, capturing, and communicating information relevant to the preparation of

reliable financial statements and the maintenance of internal control.

But effective information and communication goes beyond simply generating reports; embedded in the system should be a process for identifying and responding to the changing information and needs. Effective communication also should occur in a broader sense, flowing vertically and horizontally through the organization.

As you take a preliminary look at the state of your information and communication, consider these questions:

- How do you ensure version control on documents so that an older version is not released to the public?
- How long is the closing process for your organization, and will it allow you to meet the SEC's accelerated filing requirements? (See Appendix G for relevant dates.)
- Is there adequate time for evaluation and review of the information before it is released to the public?
- How will the shortening of public filing requirements affect your organization's ability to process information accurately?
- How will the new Form 8-K requirements (filing of significant events within four days) affect your company? A number of items now need to be disclosed, including entry into a material non-ordinary course agreement; termination of a material non-ordinary course agreement; creation of a material direct financial obligation or a material obligation under an off-balance sheet arrangement; notice of delisting or failure to satisfy a continued listing rule or standard; and more.
- Are there specific people who have the authority to disclose information to the public?

Information
Information forms the backbone of your company. Without it, you simply can't compete. Information is identified, captured, processed, and reported by information systems.

Information systems can be:

- computerized, manual, or a combination
- external, including market- or industry-specific economic data that signal changes in demand for the company's products and services; or data on goods and services the entity needs for its production process
- tailored, wherein special actions are undertaken to obtain information (e.g., questionnaires, interviews, or targeted focus groups)
- formal, delivered through periodic reports, briefings, and data
- informal, obtained through conversations with customers, suppliers, regulators, and employees, or through attendance at professional seminars

Communication
Communication can be divided into two subsets: external (i.e., the face you show to the world), and internal (i.e., your in-house means of distributing information).

Effective external communication should:

- provide external parties with an understanding of the company's policies and standards
- provide feedback to external parties as to whether internal control is effective
- enable the organization to communicate with its shareholders

In relation to internal control over financial reporting, effective internal communication should include a clear message from management that internal control responsibilities (including proper communication) are important. Up, down, and laterally, internal communication should flow unimpeded. Certain communications should not only be encouraged, but formalized. For example, there should be regular, direct communication between management and the audit committee.

Sarbanes-Oxley is also clear in its requirement that "whistleblower" provisions must be adopted. Under the law, employees must have the ability to make anonymous reports, and there can be no reprisals from communicating information that may cast the company in a negative light.

Many means of communication are available to your company, and most should be utilized in some form to provide employees with multiple options:

- policy manuals
- memoranda
- email
- voice mail
- bulletin board notices
- video messages
- group meetings

Evaluate the Design Effectiveness of Information and Communication Practices

As with other aspects of internal control, you should gain an understanding of your current state of control over information and communication before you evaluate, test, and remediate. Be aware that every company is a unique entity whose characteristics have been formed by a variety of factors, including size, industry, geography, competition, leadership, and more. Thus, what works in a Fortune 500 company may be wholly inappropriate for a small, niche company.

As part of the process, the project team should evaluate the activities that your company currently has in place to address the information and communication objectives you established earlier. From a design perspective, you need to ascertain whether the activity addresses the objective. For example, to determine whether your company communicates effectively with employees regarding their responsibilities related to internal control, look for the following activities:

- New employees that are responsible for controls that affect financial reporting receive training on the company's overall internal control processes and their specific evaluation and reporting responsibilities.
- The CFO meets at least annually with corporate controllers to discuss their role in meeting the company's objectives related to financial reporting.
- Policies, organizational charts, and operating instructions are documented and distributed to employees.

To determine whether your company's financial reporting and related application and information systems are reliable, seek evidence of the following activities:

- Procedures are in place to provide assurance that relevant information is identified, captured, processed, and reported by information systems.
- Management adequately staffs IT departments and designs the IT department to support the entity's overall business objectives.

Refer to Appendix D for a list of sample activities that address critical objectives in the information and communication component of COSO.

Test the Operating Effectiveness of Information and Communication Practices

Evidence that controls over information and communication are operating effectively may be obtained through various means:

- interviews
- self-assessment
- surveys
- inquiry
- observation
- inspection
- service organization reports

Here are a few examples of how to test the operating effectiveness of activities to address the critical information and communication objectives:

- To test the effectiveness of training programs to educate new employees who are responsible for controls that affect the financials, have a member of the project team observe a training session. This individual could also read training records to corroborate that all new employees who are responsible for controls that affect financial reporting have attended the training.
- To test the effectiveness of management's staffing of the IT department, send a survey to all IT employees asking them to rate the importance of accurate financial reporting and the department's ability to support the process of identifying, capturing, and processing financial information reported by its financial systems.
- To test the effectiveness of the company's whistleblower process, read incoming reports and the resolution of issues identified. Read presentations of information reported to the audit committee for accuracy and timeliness. Interview company employees to determine whether they are aware of the whistleblower process and whether they would use it.

Classify Design and Operating Deficiencies and Remediate

After the project team has evaluated the design and tested operating effectiveness of the company's information and communication practices, a process of prioritizing the internal control deficiencies should be conducted in a manner similar to other COSO components.

For each internal control deficiency noted, develop a remediation plan and identify the following:

- priority (high, medium, low)
- business units and locations responsible
- responsible party/function
- recommended remediation
- implementation timeframe
- estimated work effort

Communicate and obtain agreement with all parties (executive management, IT, finance function, internal audit) on the remediation plan, responsible parties, and timeframes for implementation. Remember, if the internal control deficiency is deemed a material weakness, it is imperative that the project team focus all of its efforts remediating prior to the company's assessment date and the independent auditors' internal control audit. Otherwise, it is likely that the company will receive an adverse opinion on the effectiveness of internal control over financial reporting.

3.14 Monitor the System of Internal Control

Sarbanes-Oxley requires an ongoing assessment of internal control to support your annual report on internal control. To accomplish this, you should design and deploy a process that recognizes changes in your business that impact internal control over financial reporting and each of the five components of COSO: control environment, risk assessment, control activities, information and communication, and monitoring.

Monitoring: A Primer

Monitoring essentially consists of internal control testing activities conducted over an extended timeframe. Monitoring ensures that all components of internal control operate effectively over the long haul, and makes certain that your controls keep up with the evolution of your company.

Monitoring activities can be broken into two broad categories: ongoing monitoring and separate evaluations.

Ongoing monitoring: Ongoing monitoring activities are built into the normal, recurring operating procedures of your organization. Here's an example:

Assume that, quarterly and annually, the tax manager is responsible for reviewing the deferred tax calculation and approving the journal entries to record the provision. In so doing, the tax manager has performed a control activity.

This control activity can then be integrated into a self-assessment process, wherein the tax manager's review and approval would also incorporate an evaluation of compliance with this control (i.e., was the review performed as required). This self-assessment monitoring would include, among other things, testing the effectiveness of the control and the documentation that was prepared.

In turn, this monitoring activity could be periodically validated by internal audit or another independent function.

Examples of ongoing activities include:

- routine self-assessments
- regular management and supervisory activities
- comparisons
- reconciliations
- inventory counts
- internal audit activities
- other routine actions

Separate evaluations: Separate evaluations generally take place within a limited, specified timeframe, as opposed to ongoing monitoring, which takes place continuously.

Examples of separate evaluations include:

- specific review of the controls around a process or transaction, such as "purchasing" or a significant capital expenditure
- testing a newly designed system or application
- assessment of the internal control of a business acquisition

Ongoing monitoring holds certain advantages over separate evaluations. Because it takes place in "real time," ongoing monitoring represents a proactive, rather than reactive, approach to monitoring. This allows your company to respond more rapidly to changing conditions and to detect and remediate deficiencies before they cause significant damage.

The more extensive and effective your ongoing monitoring program, the less need you will have for separate evaluations. Nonetheless, any effective monitoring system will include both types of monitoring procedures.

Also, depending on who is doing the monitoring, it may be necessary to have internal audit review the work as well.

Identify Monitoring Roles and Responsibilities

Just as with evaluating, testing, and remediating controls, monitoring can be carried out by a number of people. Divisional heads and other managers have monitoring responsibilities through continuous oversight and review. If your company has an internal audit function, it should be engaged in separate evaluations through its review activities. And internal audit itself should be evaluated periodically. The Institute of Internal Auditors recently mandated that its members undergo external quality assurance reviews every five years.

And some of the burden can be carried by employees themselves. Testing and monitoring activities can be integrated into the day-to-day job descriptions of individuals responsible for internal control. Making these activities part of the daily routine provides multiple benefits, including raising cultural awareness (control environment) of the importance of internal control; improving the likelihood of long-term sustainability; reducing the overall cost of compliance; and enhancing the deployment of company resources. Refer to Appendix E for a list of sample activities that address critical objectives in the monitoring component of COSO.

Leverage Technology for Monitoring

Monitoring can also be enhanced through the use of technology. For example, manual controls can be replaced with automated controls that are less prone to error or manipulation. And, of course, technology solutions are less susceptible or even impervious to fatigue, distraction, absenteeism, and associated problems.

3.15 Report on the Effectiveness of Controls

Ending with the End in Mind

If you started "with the end in mind," as we recommended at the beginning of this document, you are now nearing that "end" that you had in mind. It's time to prepare your internal control report.

Compile and summarize the results of your monitoring activities. If you diligently carried out the evaluation, testing, and remediation phases described earlier, then you will likely reach an inescapable conclusion: "Management believes that the company maintains effective internal control over financial reporting."

From here, your independent auditors will finalize their procedures on your controls (not just control activities, but all components of the COSO internal control framework). All of the documentation of your internal control activities that you've been assiduously compiling throughout this process should be provided to the independent auditors. Be prepared to work closely with the audit team as it works through its evaluation and testing procedures. This process will substantially differ from a financial statement audit, since it will address all five components of COSO.

Once the audit is complete, your independent auditors will issue their report. And hopefully, your efforts will come to an end and you will receive an unqualified opinion on management's assessment of internal control over financial reporting and on the effectiveness of your company's internal control over financial reporting.

Ticking Clock?

The clock is ticking. Deadlines are quickly approaching. Whether you are an early filer or a late filer, you can't afford any delay in addressing this situation.

Your company's accounting calendar will determine how much time you have left for compliance. Many companies will be required to file their initial internal control report with their first annual report on Form 10-K on or after November 15, 2004.

Accelerated 10-K and 10-Q filing schedules will exacerbate the situation. Not only does Sarbanes-Oxley impose new reporting requirements on your company, but the SEC's accelerated filing schedules for forms 10-Q and 10-K mean you will be working under a compressed timeframe. More work plus less time will equal administrative headaches for the ill-prepared.

For accelerated filers, the new 10-Q and 10-K deadlines will be phased over three fiscal years.

Fiscal Years Ending On or After	Form 10-K Deadline	Form 10-Q Deadline
December 15, 2003	75 days after fiscal year end	45 days after fiscal quarter end
December 15, 2004	60 days after fiscal year end	40 days after fiscal quarter end
December 15, 2005	60 days after fiscal year end	35 days after fiscal quarter end

To view the full text of the accelerated filing requirements, visit the SEC web site at http://www.sec.gov/rules/final/33-8128.htm.

Part Four: Appendix

Appendix A

What is Internal Control Over Financial Reporting?

In the SEC's *Final Rule on Management's Reports on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports,* the SEC has defined internal control over financial reporting as "a process designed by, or under the supervision of, the registrant's principal executive and principal financial officers, or persons performing similar functions, and effected by the registrant's board of directors, management and other personnel, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles and includes those policies and procedures that:

(1) Pertain to the maintenance of records that in reasonable detail accurately and fairly reflect the transactions and dispositions of the assets of the registrant;

(2) Provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the registrant are being made only in accordance with authorizations of management and directors of the registrant; and

(3) Provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the registrant's assets that could have a material effect on the financial statements."[24]

Appendix B

Defining Deficiencies and Weaknesses

One of the most detailed and technical areas of internal control concerns the classification of internal control deficiencies. Getting it right is critical. Confer with your independent auditors.

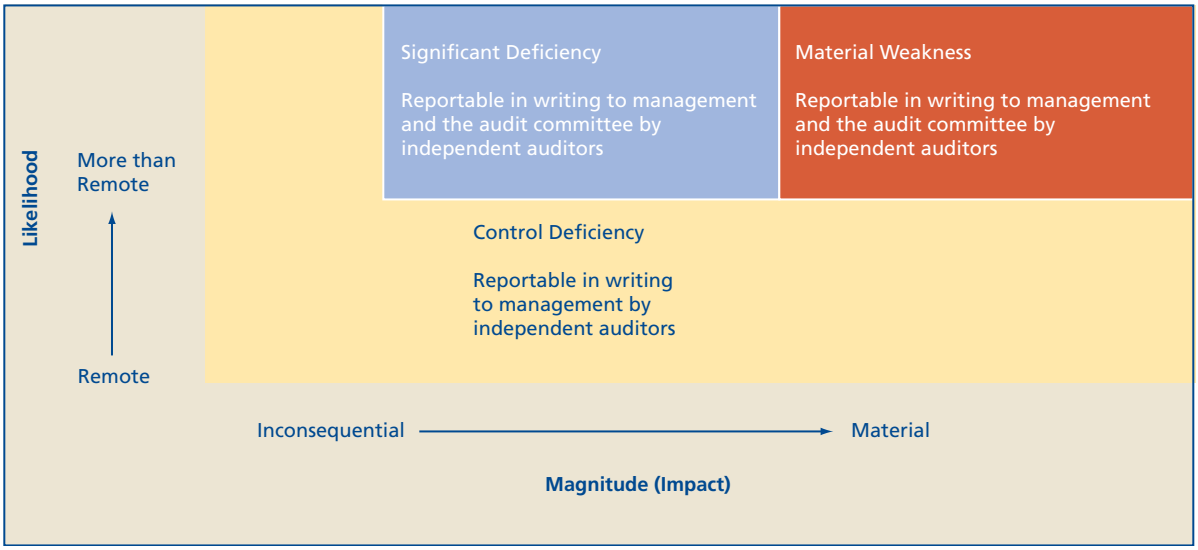
The PCAOB offers the following definitions:[25]

A ***control deficiency*** exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis. A deficiency in design exists when (a) a control necessary to meet the control objective is missing or (b) an existing control is not properly designed so that, even if the control operates as designed, the control objective is not always met. A deficiency in operation exists when a properly designed control does not operate as designed, or when the person performing the control does not possess the necessary authority or qualifications to perform the control effectively.

A ***significant deficiency*** is a control deficiency, or combination of control deficiencies, that adversely affects the company's ability to initiate, authorize, record, process, or report external financial data reliably in accordance with generally accepted accounting principles such that there is more than a remote likelihood that a misstatement of the company's annual or interim financial statements that is more than inconsequential will not be prevented or detected.

[24] "Final Rule: Management's Reports on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports," U.S. Securities and Exchange Commission, 2003. Electronic copy can be viewed at: http://www.sec.gov/rules/final/33-8238.htm.

[25] "Release No. 2004-001: Auditing Standard No. 2, An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements," Public Company Accounting Oversight Board, 2004. Electronic copy can be viewed at: http://www.pcaobus.org/rules/Release-20040308-1g.pdf.



Source: *The Proposed Auditing Standard:* An Audit of Internal Control Over Financial Reporting Performed In Conjunction With An Audit of Financial Statements

A ***material weakness*** is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the annual or interim financial statements will not be prevented or detected.

Note that management is not permitted to conclude that the company's internal control over financial reporting is effective if there are one or more material weaknesses in the company's internal control over financial reporting. As demonstrated by this chart, the severity of the deficiency increases in direct proportion to increases in the likelihood and the magnitude of a financial misstatement.

Appendix C

Sample Control Environment Objectives and Activities

Sample Objective: Through its Attitudes and Actions, Management Demonstrates Character, Integrity, and Ethical Values

Sample Activities:

- Management maintains a code of conduct and other policies regarding acceptable business practices, conflicts of interest, and expected standards of ethical behavior.
- Employees are aware of and understand the policies regarding acceptable behavior and what to do when they encounter improper behavior.
- The importance of high ethics and controls is discussed with newly hired employees through orientations or interviews.
- Management follows ethical guidelines in dealing with employees, suppliers, investors, creditors, insurers, competitors, and auditors.
- Management removes or reduces incentives or temptations that might cause personnel to engage in dishonest or unethical acts.
- Rewards, such as bonuses and stock ownership, foster an appropriate ethical tone (e.g., bonuses are not granted to those who circumvent established policies, procedures, or controls).
- When management becomes aware of departures from policies and procedures, they respond to such violations in an appropriate and timely manner.
- Any changes to established relationships with external parties (e.g., attorneys, auditors, bankers) are approved by an appropriate level of management.
- Relationships with professional third parties are periodically reviewed to establish that the entity maintains associations only with reputable third parties.

Sample Objective: The Company is Committed to Competence

Sample Activities:

- Company personnel have the competence and training necessary for their assigned duties.
- Personnel are cross-trained to understand other functions and the impact of their specific duties on other areas of the company.
- Management possesses broad functional experience (e.g., management comes from several functional areas rather than just a few, such as production and sales).
- Management consults with professionals, internal and external, in addressing significant matters relating to internal control, accounting, and financial reporting issues.

Company Documentation								
Objective	Describe activities, programs, or controls in place that are intended to satisfy the objective	Properly designed?	Describe evidence of the effectiveness of controls	Conclusion on the operating effectiveness	Deficiencies noted	Changes made during the period	Planned changes, if any	Sign off

(Re-use this template for subsequent sections.)

- Management provides personnel with access to training programs on new accounting and financial reporting issues relevant to the company.
- Formal job descriptions are in place that consider the degree to which individuals must exercise judgment and are subject to supervision.
- When an error or deficiency is detected, the cause is evaluated, and appropriate remedial actions, including training, reassignment, additional resources, or appropriate consultation, are taken on a timely basis.
- When significant changes in the business occur, the company considers the competence of the accounting and financial reporting personnel to appropriately address new issues resulting from the changes.

Sample Objective: The Audit Committee and/or the Board of Directors are Actively Involved and Have Significant Influence Over the Company's Internal Control Over Financial Reporting

Sample Activities:

- The audit committee's responsibilities are clearly articulated (e.g., in an audit committee charter), and management and the audit committee understand those responsibilities.
- The audit committee meets directly with key members of financial management, including the chief financial officer and chief accounting officer, on a periodic basis.
- The audit committee raises challenging questions with management, including questions that indicate an understanding of critical accounting policies and judgmental accounting estimates.
- The audit committee constructively challenges management's decisions, major transactions, and explanations of past results.
- The audit committee members demonstrate a willingness to call unscheduled meetings when necessary to address significant financial reporting issues.
- The audit committee members have sufficient knowledge of accounting and regulatory requirements, industry experience, and the company's business operations.
- The audit committee is independent of management and meets privately with the internal and independent auditors to discuss and challenge the reasonableness of the financial reporting and internal control process and systems.
- The audit committee reviews and approves the scope of activities of the internal and independent auditors.
- The audit committee is responsive to issues raised by the independent auditors.
- The audit committee regularly receives information from management related to key developments that may impact financial reporting.
- A process exists for the audit committee to be informed promptly and anonymously, when appropriate, of significant issues.
- The audit committee (or other committee) reviews and approves all compensation programs and considers the risks associated with various types of compensation programs (e.g., incentive-based programs may motivate management to manipulate short-term results).
- The audit committee (or other committee) specifically addresses management's adherence to the company's established code of conduct.
- The audit committee issues directives to management detailing specific actions to be taken as a result of its findings and follows up on all directives to determine that they have been properly addressed.
- The performance and effectiveness of the audit committee is periodically evaluated.

Sample Objective: Management's Philosophy and Operating Style are Consistent with a Sound Control Environment

Sample Activities:
- Management analyzes the risks and potential benefits of ventures.
- Turnover in management or supervisory personnel is monitored and the reasons for significant turnover are evaluated.
- Management regards the accounting function as a means for monitoring and exercising control over the entity's various activities.
- The central accounting and financial reporting functions have appropriate authority over decentralized accounting personnel.
- Senior management maintains contact with and consistently emphasizes appropriate behavior to subsidiary or divisional operations.
- The responsibilities and expectations for the entity's business activities and the entity's philosophy about identification and acceptance of business risk are clearly communicated to the executives in charge of those functions.
- Management exemplifies attitudes and actions reflecting a sound control environment and commitment to ethical values.
- When improper practices are reported to management, they are communicated to all appropriate parties and addressed in a thorough and timely manner.
- Management openly encourages and acknowledges the practices of employees or departments that promote a sound control environment and ethical behavior, even when the practice may be controversial.
- Management adopts accounting policies that best reflect the economic realities of the business.

Sample Objective: The Organizational Structure of the Entity is Appropriately Designed to Promote a Sound Control Environment

Sample Activities:
- The entity has defined key areas of authority and responsibility.
- The entity establishes appropriate lines of reporting, giving consideration to its size and the nature of its activities.
- The structure of the entity facilitates the flow of information across all business activities.
- Executives clearly understand their responsibility for business activities and how those business activities affect the entity as a whole.
- Reporting relationships are established to facilitate the flow of information to appropriate people in a timely manner.
- Management periodically evaluates the entity's organizational structure and makes changes as necessary based upon changes in the entity's business or industry.
- The organizational structure is not overly complex and does not include numerous or unusual legal entities.
- The business purpose of separate legal entities is evident and reasonable.
- Incompatible activities are segregated (e.g., separation of accounting for and access to assets).
- The entity has established procedures to identify related parties.
- Individuals with no apparent ownership interest in or executive position with the entity do not exercise substantial influence over the entity's affairs.

Sample Objective: The Entity Assigns Authority and Responsibility

Sample Activities:
- Employees throughout the entity are assigned authority and responsibility related to their specific job functions.
- Job descriptions contain specific references to control-related responsibilities.
- Employees are empowered, when appropriate, to correct problems or implement improvements.
- There is a structure for assigning ownership of information, including who is authorized to initiate or change transactions.
- There are policies and procedures for authorization and approval of transactions.
- Management determines and clearly communicates the responsibilities and expectations of the finance and accounting departments.

Sample Objective: Human Resource Policies and Procedures

Sample Activities:
- Management establishes and enforces standards for hiring the most qualified individuals, with emphasis on educational background, prior work experience, past accomplishments, and evidence of integrity and ethical behavior.
- Recruiting practices that include formal, in-depth employment interviews and informative, insightful presentations on the entity's history, culture, and operating style demonstrate the entity's commitment to its employees and its attitude toward a sound control environment.
- Training policies communicate prospective roles and responsibilities and illustrate expected levels of performance and behavior.
- Rotation of personnel and promotions that are driven by periodic performance appraisals demonstrate the entity's commitment to the advancement of qualified personnel to higher levels of responsibility.
- Disciplinary actions send a message that violations of expected behavior will not be tolerated.
- An ongoing education process enables people to deal effectively with evolving business environments.

Appendix D

Sample Information and Communication Objectives and Activities

Sample Objective: Financial Reporting and Related Application and Information Systems are Reliable

Sample Activities:
- Management has a strategic plan for information systems that is linked to the entity's overall strategies. The objectives of the IT plan include the preparation of high-quality financial reports for external use and consideration of the accounting department's needs.
- Procedures are in place to provide assurance that relevant information is identified, captured, processed, and reported by information systems in an appropriate and timely fashion.
- Control activities are in place to ensure the accuracy and integrity of data forming the basis for reports.
- Management adequately staffs the IT department and designs the IT department to support the entity's overall business objectives.
- Management monitors user satisfaction with information provided (e.g., management monitors the frequency and nature of requests to change information).

Sample Objective: Appropriate and Necessary Information is Obtained from, and Provided to, Management

Sample Activities:
- Management monitors relevant external information.
- Internal information regarding financial results is generated by the entity's financial information systems and that information is reported regularly.
- Entity-wide operating results are reviewed and compared against budgets at regular intervals.
- The adequacy of the information technology structure is considered by senior management.
- There is a process for decentralized operations or departments to request changes to reports either generated by the accounting function or automatically generated by the system.
- If a number of requests are received to change reports, the reasons for such requests are examined and the reports are changed as determined necessary.
- Managers and personnel at various levels are interviewed or surveyed to determine the information that is needed or desired throughout the organization.
- Management monitors the reasons that personnel create ad hoc reports.

Sample Objective: Information is Gathered from and Disseminated to the Appropriate People on a Timely Basis

Sample Activities:
- Managers receive analytical information so they can identify necessary actions to be taken.
- Financial controllers meet periodically with line management to discuss operational results.
- Information is provided in sufficient detail, varying for the different levels of management.
- Financial controllers receive an appropriate amount of detailed information when reviewing financial results.
- Information is provided in a timely enough manner to allow for effective monitoring.
- There are established and agreed upon deadlines for period-end reporting and the deadlines allow for an appropriate review by senior officers and management.
- Information provided is relevant and accurate.

Sample Objective: There is a Timely Process for Identifying and Responding to the Changing Information and Communication Needs

Sample Activities:
- There is a mechanism for identifying emerging information needs.
- The entity has a process to address information needs arising from new accounting standards.
- Management devotes substantial time to the consideration of information systems needs for the accounting and controlling functions.
- Management understands the information systems needs as they relate to financial reporting.
- The entity-level resources devoted to information systems for financial reporting are appropriate in relation to resources devoted to other areas of the entity.
- Management establishes indicators to assess the appropriateness of the financial information systems.

Sample Objective: The Entity Effectively Communicates the Employees' Responsibilities Related to Internal Control

Sample Activities:
- Management communicates authorities across the organization.
- Management uses training, meetings, or on-the-job supervision to communicate financial reporting and internal control matters.

- New employees in the corporate accounting department are required to attend training regarding their role in the internal control structure and how it affects others.
- Employees know the objectives of the company as related to financial reporting and how their activities affect those objectives.
- The CFO or person in a similar position meets with corporate controllers, at least annually, to discuss their role in meeting the company's objectives related to financial reporting.
- Policies, organization charts, and operating instructions are documented and distributed to employees.
- Employees know how their activities interact with the duties of other employees.
- Employees responsible for financial reporting at the entity-level periodically discuss the company's objectives and each person's role in meeting those objectives.

Sample Objective: A "Whistleblowing" Program Has Been Established, and Management's Reaction is Monitored as it Relates to Financial Reporting

Sample Activities:
- There is a means for employees to communicate upstream, anonymously if so desired, other than through a direct supervisor.
- There is a means for third parties to communicate financial reporting issues, anonymously if so desired.
- The communication channels established by management or the audit committee have been used in the past.
- Problems have been reported and resolved appropriately in the past.
- Reported problems are investigated in a timely manner and disciplinary actions are taken when necessary.
- All financial reporting improprieties are communicated to the audit committee.
- Positive feedback is provided to employees that report suspected problems.
- Management does not impose retribution on employees that report improprieties.
- There are realistic mechanisms in place for employees to provide recommendations.
- Management positively recognizes personnel who take an ethical stance.

Sample Objective: Management's Communication Across and Outside the Company Reflects an Attitude Toward Sound Internal Control

Sample Activities:
- There is communication throughout the organization about the company's entity-wide objectives regarding financial reporting.
- The CFO or a person in a similar position meets regularly with divisional management to communicate expectations regarding financial reporting objectives for the company as a whole.
- Management communicates to personnel and other parties that a sound system of internal control is a priority of the company.

Appendix E

Sample Monitoring Objectives and Activities

Sample Objective: Internal Audit's Scope, Responsibilities, and Audit Plans are Appropriate for the Company

Sample Activities:
- The scope of internal audit's activities are reviewed in advance with management, the audit committee, and the independent auditors.
- Internal audit has appropriate levels of staff to execute their plans.
- Internal audit has the authority to review any aspect of the entity's operations.
- The audit plan is responsive to the entity's risk assessment.
- The internal audit personnel are experienced and competent.
- Monitoring controls are reviewed to ensure that they are being applied as expected.

Sample Objective: Internal Audit Adheres to Professional Standards, Such as Those Issued by The Institute of Internal Auditors

Sample Activities:
- Internal audit is independent of the activities that they audit.
- Internal audit has direct access to the audit committee and the board of directors.
- Internal auditors are prohibited from having an operating role in the activities that they monitor.
- Internal audit is evaluated by an external party.
- There is a defined reporting process for progress and results.

Sample Objective: The Entity is Responsive to Internal and External Recommendations

Sample Activities:
- Executives with proper authority decide which of the internal and independent auditors' recommendations will be implemented.
- Management takes appropriate action on exceptions to policies and procedures.
- Action plans are implemented and there is follow-up to verify implementation.
- Management is required to respond, on a timely basis, to the internal audit department's findings and recommendations, or questions on financial results and variances from budget. Responses to internal or external audit findings are provided to the audit committee or board of directors.
- Corporate accounting personnel investigate and respond accordingly to financial reporting issues identified at subsidiary levels.
- Management responds, in writing, to concerns raised in the management letter. The audit committee requires divisional or subsidiary management letters to be provided to them, with written responses from divisional or subsidiary management.
- Recommendations for improvements are adopted and deficiencies noted have been remediated.
- Management responds timely to comments identified in the management letters.

Sample Objective: Communications from External Parties

Sample Activities:
- Complaints of improper financial matters by external parties such as suppliers or regulators are fully investigated and documented (e.g., disputes over inappropriate shipping charges or bill and hold practices by customers are investigated by management).
- Reported improprieties from individuals other than employees are investigated and resolved.
- Discrepancies that have been identified by customers are investigated and resolved.
- Communications from vendors and monthly statements of accounts payable are used as a control monitoring technique.
- Management utilizes proactive controls regarding third-party information (e.g., vendor confirmations).
- Controls that should have prevented or detected problems are reassessed when problems occur.

Sample Objective: Internal Meetings are an Effective Means of Providing Feedback to Management on Whether Controls are Operating Effectively

Sample Activities:
- Relevant issues and questions that are raised at training seminars are captured.
- Employee suggestions are communicated upstream and acted on as appropriate.
- Management uses surveys and focus groups to understand employee perceptions.

Sample Objective: Self-Assessments

Sample Activities:
- Personnel are required to acknowledge compliance with the code of conduct.
- Signatures are required to verify performance of significant control functions such as reconciliations.
- The results of self-assessments regarding the company's code of conduct and significant control activities are independently verified.
- The personnel that perform self-assessments regarding the control activities being performed by process owners complete the self-assessment based on "first-hand knowledge" of control activities that they have observed.
- Operating personnel are required to "sign off" on the accuracy of their unit's financial statements. Internal management reports are reviewed and initialed by operating personnel to verify accuracy. In addition, these reports are reconciled to any external financial reports.
- Policies and procedures ensure that appropriate personnel perform a detailed review of operating and financial information to ascertain the integrity of the information (e.g., advertising personnel review the monthly advertising expenses to ensure that they are consistent with the authorized payments).

Sample Objective: Separate Evaluations

Sample Activities:
- Personnel with the requisite skills conduct evaluations of appropriate portions of the internal control system.
- The scope, depth of coverage, and frequency of evaluations are adequate.
- The frequency and scope of supervision and monitoring activities are appropriate to the size and nature of the entity.
- Supervisory personnel perform various random and structured reviews over the functioning of control procedures.
- Personnel with the requisite skills and independence of function periodically evaluate appropriate areas of the internal control structure.
- An analysis is made using the evaluation results compared to established criteria.
- The methodology for performing separate evaluations includes checklists, questionnaires, or programs.
- The evaluation team is brought together to plan the evaluation process and ensure a coordinated effort.
- An executive with requisite authority manages the evaluation process.
- The results of the evaluation and action plans are documented.

Appendix F

COSO — The Sequel

In 2002, COSO announced that it had launched a study designed to provide guidance in helping organizations manage risk. The study resulted in the release for public comment of *Enterprise Risk Management Framework*. The proposed framework details essential components and concepts of enterprise risk management for all organizations, regardless of size.

Enterprise Risk Management Framework is not intended to replace COSO's *Internal Control — Integrated Framework* as a framework for internal control. Enterprise risk management is broader than internal control and, therefore, the new publication expands on the concepts of the original to focus more fully on the management of risk. Observers expect this new enterprise risk management framework to provide common terminology and become the most widely adopted model for risk management.

A draft copy of *Enterprise Risk Management Framework* may be viewed at:
http://www.erm.coso.org/Coso/coserm.nsf/frmWebCOSOHome?ReadForm.

Appendix G

Not Sure if You are an Accelerated Filer?

Any company that is an "accelerated filer" must comply with the provisions of section 404 as of the end of its first fiscal year ending on or after November 15, 2004. Don't know if you're an accelerated filer? According to the SEC, accelerated filers are, generally, U.S. companies that have equity market capitalization over $75 million as of the last business day of its most recently completed second fiscal quarter and have filed an annual report with the SEC. For purposes of determining whether a company meets the market value requirements of $75 million, the market test must be conducted annually until the requirements are met. For example, a calendar year-end company that did not meet the market value test on June 30, 2003, will be required to conduct a market test on June 30, 2004. If it meets the market test and the other accelerated filer requirements on that date, it will be classified as an accelerated filer and will be required to comply with the requirements of section 404 as of December 31, 2004 (its first fiscal year ending after November 15, 2004).

About Deloitte
Deloitte, one of the nation's leading professional services firms, provides audit, tax, consulting, and financial advisory services through nearly 30,000 people in more than 80 U.S. cities. Known as an employer of choice for innovative human resources programs, the firm is dedicated to helping its clients and its people excel. "Deloitte" refers to the associated partnerships of Deloitte & Touche USA LLP (Deloitte & Touche LLP and Deloitte Consulting LLP) and subsidiaries. Deloitte is the U.S. member firm of Deloitte Touche Tohmatsu. For more information, please visit Deloitte's Web site at www.deloitte.com/us.

Deloitte Touche Tohmatsu is an organization of member firms devoted to excellence in providing professional services and advice. We are focused on client service through a global strategy executed locally in nearly 150 countries. With access to the deep intellectual capital of 120,000 people worldwide, our member firms, including their affiliates, deliver services in four professional areas: audit, tax, consulting, and financial advisory services. Our member firms serve more than one-half of the world's largest companies, as well as large national enterprises, public institutions, locally important clients, and successful, fast-growing global growth companies.

Deloitte Touche Tohmatsu is a Swiss Verein (association), and, as such, neither Deloitte Touche Tohmatsu nor any of its member firms has any liability for each other's acts or omissions. Each of the member firms is a separate and independent legal entity operating under the names "Deloitte," "Deloitte & Touche," "Deloitte Touche Tohmatsu," or other, related names. The services described herein are provided by the member firms and not by the Deloitte Touche Tohmatsu Verein. For regulatory and other reasons, certain member firms do not provide services in all four professional areas listed above.

#4139