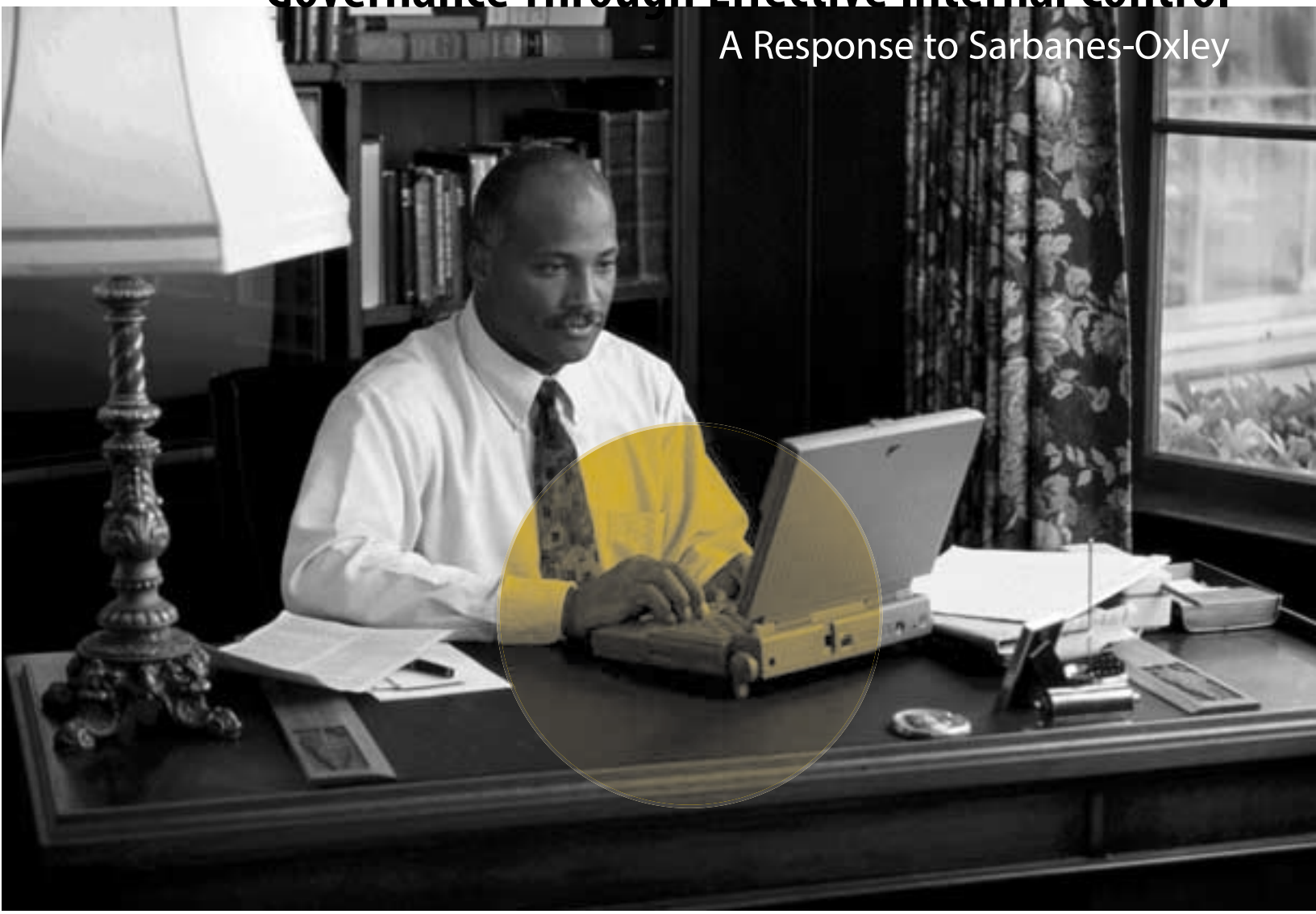
Deloitte & Touche

Moving Forward–A Guide to Improving Corporate Governance Through Effective Internal Control

A Response to Sarbanes-Oxley



Note to Readers Regarding This First Edition – January 2003:

This document was published before the SEC had fully promulgated its Sarbanes-Oxley rules. As a result, subsequent actions by the SEC may substantially alter the accuracy and validity of the material presented herein. Contact your Deloitte & Touche advisor for more information.

Moving Forward

A Guide to Improving Corporate Governance Through Effective Internal Control: A Response to Sarbanes-Oxley

Table of Contents

Executive Summary

The Sarbanes-Oxley Act of 2002 has literally rewritten the rules for corporate governance, disclosure, and reporting. Yet beneath the act's myriad pages of legalese lies a simple premise: Good corporate governance and ethical business practices are no longer niceties — *they are the law*.

Internal Control

Recent business scandals have found executives testifying that they were "unaware" of dubious activities — off-the-book partnerships, improper revenue recognition, etc. — carried on by their companies. Sarbanes-Oxley aims to discourage such claims through a number of measures that will strengthen internal checks and balances and enhance accountability.

Most notably, Sarbanes-Oxley focuses heavily on the critical role of "internal control." Internal control is a process effected by a company's board of directors, management, and other personnel that drives business success in three categories:

- effectiveness and efficiency of operations;
- reliability of financial reporting;
- compliance with applicable laws and regulations.

Sarbanes-Oxley makes CEOs and CFOs explicitly responsible for establishing, evaluating, and monitoring the effectiveness of internal control over financial reporting and disclosure.

The new and proposed SEC rules that effect Sarbanes-Oxley are undeniably complicated, and implementation will be both time-consuming and costly, but there are a few mitigating factors:

1. Virtually all public companies already have some semblance of an internal control structure in place, although it may be informal and not sufficiently documented.
2. Many companies will be able to tailor existing processes to comply with the internal control provisions of Sarbanes-Oxley.
3. Setting up a strong internal control structure to meet the mandates of the act can provide benefits well beyond compliance. Indeed, the potential to revise and realize new corporate visions and achieve new levels of corporate excellence abounds.

Some observers have described Sarbanes-Oxley as the most significant piece of business legislation in the last half-century. The point may be arguable, but this fact is not: Sarbanes-Oxley fundamentally changes the business and regulatory environment, and public companies can't afford to underestimate the task ahead. The clock is ticking on compliance and any delays in dealing with the issue may have serious consequences. Immediate and decisive action is required.

Critical Sections

Much of the discussion surrounding Sarbanes-Oxley has focused on Sections 302 and 404, as will this publication.

Under **Section 302**, CEOs and CFOs must *personally* certify that they are responsible for disclosure controls and procedures. Each quarterly filing must contain a certification that they have performed an evaluation of the design and effectiveness of these controls. The certifying executives must also state that they have disclosed to their audit committee and independent auditor any significant control deficiencies, material weaknesses, and acts of fraud. The SEC has also proposed an expanded certification requirement that includes internal controls and procedures for financial reporting, in addition to the requirement related to the disclosure controls and procedures.

Section 404 mandates an annual evaluation of internal controls and procedures for financial reporting. In addition, the company's independent auditor must issue a separate report that attests to management's assertion on the effectiveness of internal controls and procedures for financial reporting.

Steps Toward Developing an Internal Control Program

We recommend the following steps for developing an internal control program to address these provisions of Sarbanes-Oxley:

1 *Start With the End in Mind*

Some companies have adopted a strategy that prioritizes compliance with Section 302 over that of Section 404, under the rationalization that Section 302 is already in force and Section 404 won't apply until late 2003. Yet we believe that separately addressing these two sections of the act constitutes an inefficient process. Quite simply: *The mandates of both sections can be addressed through a single methodology*.

2 *Commit and Organize*

Understanding how Sarbanes-Oxley applies to your company — based on its business characteristics — can aid in the development of your internal control program. Many factors will come into play. For example, larger companies will face challenges distinct from those of smaller enterprises. Also, the extent to which you already have a strong internal control framework in place will have significant bearing on your activities.

Three groups will play a prominent role: the **board of directors,** which oversees the company's commitment to the task; the **CEO and CFO**, who acknowledge responsibility for ensuring compliance and communicate this information to key management and employees; and the **steering committee,** which oversees and coordinates Sarbanes-Oxley activities across the organization.

3 *Select a Suitable Internal Control Framework*

To meet the objectives of the act, many companies build their internal control structure around the recommendations of the Committee of Sponsoring Organizations of the Treadway Commission (COSO). While other frameworks for internal control exist, we believe COSO will become the dominant model, and we recommend its adoption.

The COSO framework breaks effective internal control into five interrelated components:

>Control Environment – the foundation for all other elements of internal control, which includes the ethical values and competence of the company's employees.

>Risk Assessment – the identification and analysis of relevant risks that can hinder the achievement of business objectives.

>Control Activities – specific tasks to mitigate each of the risks identified above.

>Information and Communication – information pathways from management to employees and vice versa.

>Monitoring – the evaluation and assessment of internal control.

4 *Empower the Disclosure Committee*

The formation of a disclosure committee represents one of the most important controls that a company can implement. The disclosure committee performs numerous functions, including reviewing SEC filings, recommending parameters for disclosure, overseeing disclosure processes, and reviewing control deficiencies and material weaknesses with the CEO and CFO.

5 *Establish an Internal Control Program*

For this labor-intensive step, a number of actions are required:

>Plan the Project – We recommend forming an internal control program management team to establish or strengthen the internal control program. Smaller enterprises may be able to redeploy, on a part-time basis, existing staff. Larger companies may need dedicated full-time personnel.

>Assess the Control Environment – Forming the foundation of internal control, the control environment includes such elements as integrity, ethical values, and competence; management's philosophy and operating style; delegation of authority and responsibility; and the direction provided by the board of directors. A cultural assessment can aid in understanding and documenting your existing control environment.

>Define the Scope – The goal of the scope definition process is to identify financial reporting and disclosure risks. This will allow efforts to be prioritized and focused.

>Build a Controls Repository – The controls repository serves as a clearinghouse for all information and activities related to internal control, containing docu-

mentation on control objectives, design, and implementation as well as methods for testing the operating effectiveness of such activities.

>Perform Initial and Ongoing Tests – The operating effectiveness of the control activities should be evaluated by various parties, including the individuals responsible for the controls and the internal control program management team.

>Monitor – The internal audit function should monitor the effectiveness of the entire internal control program and infrastructure. (Companies without an internal audit function may consider using the internal control program management team to perform these activities.)

Enabling Technologies to Achieve Results

A variety of tools can aid in the development of an internal control program. Database programs and proprietary tools can be used to document control objectives, processes, and activities; can help to identify gaps and track actions to remediate deficiencies; and can support self-assessment and monitoring activities.

Conclusion

Parallels can be drawn between the effect of the Sarbanes-Oxley Act of 2002 on public companies and the impact of the Federal Deposit Insurance Corporation Improvement Act of 1991 (FDICIA) on the banking industry: Both statutes introduced regulations to remedy perceived market failures and each enacted significant new reporting requirements. There are several lessons public companies can learn from the FDICIA example.

1. **Accept that the environment has profoundly changed.** Companies must recognize that they operate in a new environment — one that demands more effort and accountability.
2. **Promote understanding of internal control within the organization.** Companies may be tempted to show superficial compliance with Sarbanes-Oxley, but such an approach may backfire if controls fail because form was stressed over substance.
3. **Factor into your business model the cost of developing an internal control program.** Good internal control is not a one-time expense; rather, it fundamentally changes the cost of doing business.

Recent events have placed us in a unique period in the history of American business. The call for corporate responsibility has never been greater. The need to link sound corporate governance to effective control activities has never been clearer. And in terms of restoring public confidence in the financial markets, there has never been more at stake. Forward-thinking companies and executives will seize the opportunity. Those who fail to act may pay a heavy price.

Moving Forward

Obligations and Opportunities

In July 2002, President George W. Bush signed the Sarbanes-Oxley Act into law and into the collective consciousness of business leaders and government officials around the world. Replete with accounting, disclosure, and corporate governance reforms, this statute seeks, in tangible ways, to "repair" the public's lost faith in our country's business leaders, and to re-emphasize the importance of ethical standards in the preparation of financial information reported to investors.

Sarbanes-Oxley and related rules issued by the Securities and Exchange Commission are complex laws and regulations that have engendered confusion and consternation in the business community. But behind all the rules and requirements, the certification of "this" and the attestation to "that," the Sarbanes-Oxley Act is simply government's way of putting legal teeth into the basic precepts of *good corporate governance and ethical business practices*. Sarbanes-Oxley codifies the view that company management should be aware of material information that is filed with the SEC and released to investors, and should be held accountable for the fairness, thoroughness, and accuracy of this information.

Many observers believe that instituting these new procedures for internal control and executive certification represents an essential course correction for public companies, mandating processes that companies should have considered adopting in the first place. Similarly, other pundits contend that focusing on good corporate governance and transparency of financial information simply makes sound business sense. But the new rules come at a cost: These changes will necessitate significant alterations in the procedures and practices, as well as the day-to-day lives, of many senior executives and the people reporting to them. Yet most companies won't need to start from scratch: Many will be able to tailor their existing processes to comply with the internal control requirements of Sarbanes-Oxley.

Perhaps the most important realization is that the playing field has changed dramatically — and permanently. For a public company, compliance under Sarbanes-Oxley is non-negotiable; if you are "unhappy" with the provisions, you can't simply pick up your ball and go home. (Unless, of course, you choose an alternative strategy — taking your company private.) For audit committees and senior management of public companies, particularly CEOs and CFOs, the definitions of financial stewardship and personal accountability have been made more explicit and the stakes significantly higher.

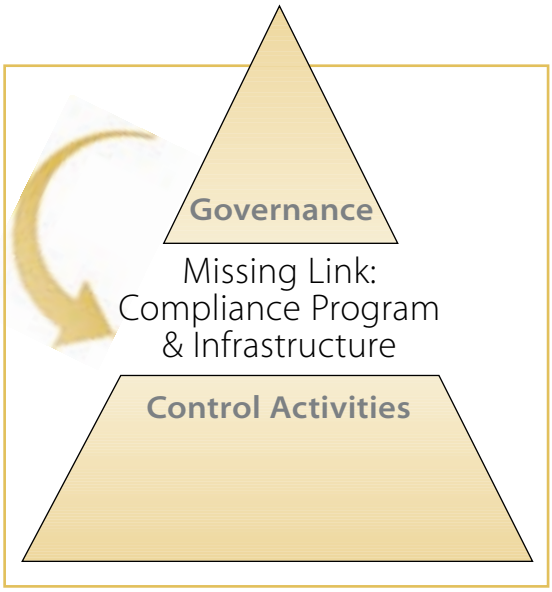
Your obligations are clear but so are your opportunities. By effectively navigating this new landscape, *the potential to revise and realize new corporate visions and achieve new levels of corporate excellence abounds*. Forward-thinking executives will endeavor to harness the mandated changes to drive better business performance.

Private companies, although not legally obligated to comply with the act, may also choose to adopt certain components as part of an overall plan to improve business operations.

This document focuses heavily, as does Sarbanes-Oxley itself, on internal control. But readers should be aware that internal control makes up just one of the many components of good corporate governance. Numerous other considerations also come into play: integrity and ethical values; management philosophy and operating style; organizational structure; well-delineated roles and responsibilities for boards, management, and employees; commitment to excellence; effective and proactive boards and committees; and many more.

As a steward of your company, it behooves you to treat Sarbanes-Oxley compliance as a top priority. This new emphasis on internal control and transparent disclosure is no passing fad. Sarbanes-Oxley fundamentally changes your world, and you can't afford to underestimate the task before you. Immediate action is required.

Many of the provisions of the act are still in their formative stages, and new rules and regulations will be promulgated. Undoubtedly, the effects of the Sarbanes-Oxley Act will be felt well into the future.



Linking Governance To Control Activities

The Sarbanes-Oxley Act makes company executives explicitly responsible for establishing, evaluating, and monitoring the effectiveness of their company's internal control structure. For many executives, the intricacies of compliance and the implications of failure can be daunting.

Yet the situation may not be as dire as imagined. That's because almost every public company *already has in place* some semblance of an internal control structure. For example, whenever a member of the finance department uses a unique password to gain access to the company's financial system, a control is being exerted.

Furthermore, most companies *already have implemented* some level of monitoring. For instance, using the example above, whenever a supervisor reviews the user logs to determine that appropriate system access is being maintained, monitoring is taking place.

Yet while the situation may not be dire, it may be far from optimal. At many companies, a significant gap exists between the employees performing control activities and the executives who make strategic governance decisions.

Defining Controls

Certain terms related to internal control arise frequently during discussion of the Sarbanes-Oxley Act and associated SEC regulations. Here are brief definitions of the most commonly used.

Internal Control

The most widely accepted definition of internal control was developed by the Committee of Sponsoring Organizations of the Treadway Commission:

"… a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- effectiveness and efficiency of operations;
- reliability of financial reporting;
- compliance with applicable laws and regulations."

Internal Controls and Procedures for Financial Reporting

The SEC has proposed defining internal controls and procedures for financial reporting to mean "controls that pertain to the preparation of financial statements for external purposes that are fairly presented in conformity with generally accepted accounting principles."

Disclosure Controls and Procedures

A term newly introduced by the SEC following the enactment of Sarbanes-Oxley, disclosure controls and procedures "are designed to ensure that information required to be disclosed by a company in the reports filed by it under the Exchange Act is recorded, processed, summarized, and reported within the time periods specified by the SEC." This definition includes both financial and non-financial disclosures.

Examples of non-financial disclosure may include such items as the signing of a significant contract; developments regarding intellectual property; changes in union relationships; termination of a strategic relationship; legal proceedings; or required disclosures in the Management's Discussion and Analysis contained in Forms 10-K, 10-Q, and 20-F.

Most companies do not — nor, before Sarbanes-Oxley, were they legally obliged to — have a direct link from the governance activities of the board and senior management to the control activities of the organization. But now, because Sarbanes-Oxley requires top executives to state, for the record, how well their internal control structure is functioning, establishing such a link is crucial to compliance.

A strong internal control structure can provide benefits well beyond compliance with Sarbanes-Oxley.

The purpose of this document is to provide an overview of an internal control program and infrastructure that companies can tailor to mesh with existing resources, processes, and technologies, and to provide the missing link that connects strong control activities with responsive corporate governance. On the following pages, we will summarize — in plain English — Sections 302 and 404 of Sarbanes-Oxley and some potential ramifications for your company. We will recommend committees to form, principles to observe, and information to capture, and will help map — step-by-step — a path leading to an enhanced internal control structure.

The benefits may extend far beyond compliance with Sarbanes-Oxley. In fact, a strong internal control structure can help your company:

- make better business decisions with higher quality, more timely information;
- gain (or regain) investor trust;
- prevent loss of resources;
- comply with applicable laws and regulations;
- gain competitive advantage through streamlined operations.

Conversely, the consequences of failure could be nothing short of disastrous. Companies that neglect to institute the required controls may find themselves in situations similar to those that led to the promulgation of Sarbanes-Oxley in the first place, resulting in:

- increased exposure to fraud;
- sanctions from the SEC;
- unfavorable publicity;
- negative impact on shareholder value;
- shareholder lawsuits or other legal actions.

We recommend that, after reading this document, you consult with legal counsel and your independent auditor to discuss the development of an internal control program customized to your business.

Step 1
Start With the End in Mind

To enhance performance, many professional athletes visualize the perfect shot or the perfect swing. This technique can well serve here.

Visualize what your company will look like after your internal control program is operating smoothly:

Imagine...

- *... a strong internal control framework that helps keep your company on course toward growth and profitability.*
- *... procedures that allow you to meet significant new reporting and disclosure requirements mandated by Sarbanes-Oxley.*
- *... a framework that withstands the scrutiny of your independent auditor, the SEC, and other regulatory bodies.*
- *... increased investor confidence in your company.*
- *... your company becoming a recognized leader in corporate governance, known for the quality and integrity of its financial reporting.*
- *... improved flow of information permitting better business decisions.*
- *... a restoration of trust and confidence in the public securities market that was earned by corporate executives because they took this process seriously and responsibly.*

Much of the discussion — and the uncertainty — surrounding Sarbanes-Oxley has focused on Sections 302 and 404, and rightly so.

Many companies have adopted a strategy that prioritizes compliance with Section 302 over that of Section 404. Ostensibly, such an approach makes sense. After all, Section 302 is already in force (since August 2002), whereas Section 404, as proposed, won't apply until late 2003.

Yet we believe that separately addressing these two sections of the act constitutes an inefficient and likely counterproductive process. Solid arguments can be made for integrating the provisions of each into a larger internal control structure robust enough to comply with *both* Sections 302 and 404. We'll outline that rationale below. But first, a brief summary of each section of the act will help to clarify the discussion.

Section 302: Your Quarterly and Annual Certification of Disclosure Controls and Procedures

Section 302 imposes new levels of accountability on CEOs and CFOs, who now must *personally* certify that disclosure controls and procedures have been implemented and evaluated. (The SEC has also proposed an expanded certification requirement that includes internal controls and procedures for financial reporting, in

Section 906: Corporate Responsibility for Financial Reports

Another widely publicized provision of Sarbanes-Oxley — Section 906 — took effect in August 2002. This section requires CEOs and CFOs to sign and certify the periodic report containing financial statements. The executive certification states that the report complies with SEC reporting requirements and fairly represents the company's financial condition and the results of its operations. Failure to comply with this requirement carries a high price: Fines of up to $5 million and imprisonment for up to 20 years can be imposed for knowing or willful failure to comply. This is the provision that carries the "teeth" of the act.

addition to the requirement related to disclosure controls and procedures.) Roles have been altered as well: The CEO must now directly acknowledge responsibility for internal control that previously had been largely delegated to the CFO.

With each quarterly and annual filing, the CEO and CFO must certify that they:

- are responsible for disclosure controls and procedures;
- have designed (or supervised the design of) these controls to ensure that material information is made known to them;
- have evaluated the effectiveness of these controls each quarter;
- have presented their conclusions regarding the effectiveness of these controls;
- have disclosed to their audit committee and the independent auditors any significant control deficiencies, material weaknesses, and acts of fraud that involve management or other employees who have a significant role in the company's internal control;
- have indicated in the filing any significant changes to controls.

Meeting some of the mandates of Section 302 may prove relatively painless. For example, reaffirming each quarter that the CEO and CFO are responsible for disclosure controls and procedures may quickly become a regular task. Yet the simple wording of other provisions belie the level of effort that may be required to comply. Consider, for example, the requirement that disclosure controls and procedures be reevaluated every quarter. For a dynamic organization that is creating new products and services, completing mergers and acquisitions, forming alliances, and reorganizing divisions and departments, the sheer logistics of developing, monitoring, and evaluating such controls can rapidly become daunting.

Section 404: Your Annual Assessment of Internal Controls and Procedures for Financial Reporting

Section 404 mandates an annual evaluation of internal controls and procedures for financial reporting. Like Section 302, Section 404 requires CEOs and CFOs to periodically assess and vouch for the effectiveness of these controls.

Section 404 obliges companies to include in their annual report an internal control report from management that:

Defining Deficiencies and Weaknesses

Control Deficiency: A "control deficiency" indicates a flaw in the design, the implementation, and/or the operating effectiveness of a control activity. Such defects could adversely affect the company's ability to initiate, record, process, summarize, and report accurate financial and non-financial data.

Significant Deficiency/Reportable Condition: The SEC's description of a significant deficiency makes it analogous to a "reportable condition" as described in the auditing standards. Reportable conditions are control deficiencies coming to the independent auditor's attention that, in his or her judgment, should be communicated to the audit committee because they represent significant deficiencies in the design or operation of internal control, which could adversely affect the organization's ability to initiate, record, process, summarize, and report accurate financial data and non-financial data.

Material Weakness: According to auditing standards, a material weakness is a reportable condition in which the design or operation of one or more of the internal control components does not reduce to a relatively low level the risk that misstatements caused by error or fraud in amounts that would be material in relation to the financial statements being audited may occur and not be detected within a timely period by employees in the normal course of performing their assigned functions. Evaluating whether a reportable condition is also a material weakness is a subjective process that depends on factors such as the nature of the accounting system and of any financial statement amounts or transactions exposed to the reportable condition, the overall control environment, other controls and the judgment of those making the decision. The presence of one or more material weaknesses may indicate that the internal control structure is not effective.

- affirms their responsibility for establishing and maintaining internal controls and procedures for financial reporting;
- evaluates and reaches conclusions about the effectiveness of internal controls and procedures for financial reporting;
- states that the company's independent auditor has attested to, and reported on, management's evaluation of the company's internal controls and procedures for financial reporting.

Under the proposed SEC rules, management will also be required to certify the effectiveness of their internal controls and procedures for financial reporting on a quarterly basis.

In addition, Sarbanes-Oxley requires a company's independent auditor to complete a separate report that attests to *management's assessment* of the effectiveness of internal controls and procedures for financial reporting.

Because your company's CEO and CFO must make public statements regarding the effectiveness of internal control, substantial support and documentation regarding both your internal control structure and your evaluation should be maintained. Also, because your independent auditor will be attesting to *your evaluation* of your controls, you should be prepared to provide this documentation to them.

Be aware that a "clean" opinion in your last financial statement audit isn't a testament to the effectiveness of your internal control. When your independent auditors rendered an opinion on your financial statements, they were not attesting to your internal control structure; therefore, the testing procedures they performed were not designed to meet the attestation requirements.

In order for your independent auditor to carry out this attestation — and for you to prepare your own assessment — you should adopt an internal control framework that contains objective criteria that can be measured and evaluated. We believe that the recommendations of the Committee of Sponsoring Organizations of the Treadway Commission (COSO) will emerge as the most frequently used framework by registrants.

The evaluation that you provide to your independent auditors should be substantive, well documented, and comprehensive. An abbreviated checklist may include:

- information about your company's overall control environment;
- description of the process undertaken by management to identify, classify, and assess risks that would prevent the company from achieving its financial reporting objectives;
- complete description of the control objectives created by management to address the risks identified and the related control activities;
- description of the information systems and communication procedures in place to support the above;
- results and underlying documentation of management's latest evaluation of the design and operating effectiveness of individual control activities (note: reliance solely on representations of subordinates may not suffice);
- listing of all deficiencies found in the design and implementation of control activities, as well as proposed remediation procedures;
- description of the process to communicate significant deficiencies and material weaknesses to the independent auditors and audit committee;
- description of the monitoring procedures to ensure that the internal control structure is functioning as intended and the results of the monitoring procedures are reviewed and acted upon;
- description of the disclosure creation process and related control activities.

302 Plus 404 Equals 1

Now, armed with a more comprehensive understanding of Sections 302 and 404, an effective strategy becomes clear: *The mandates of both sections can be addressed through a single methodology*. An internal control program that simultaneously focuses on disclosure and financial reporting can meet the quarterly requirements of Section 302, the annual requirements of Section 404, as well as the needs of independent auditors to perform their attestation procedures. (A call to more closely align the requirements of the two sections of Sarbanes-Oxley has echoed

throughout the business community, and most observers expect the SEC to continue to move in that direction.)

Effective, yes, but easy? Not at all. The tasks are many: This new emphasis on internal control and compliance must be infused throughout the organization. Smaller companies, which most likely don't have a robust infrastructure and an extensive staff, may find conformity especially taxing. Companies of all sizes will be forced to devote significant resources to the effort — time, money, and personnel.

The dollar costs of compliance will be considerable (but not, it should be noted, as high as the costs of non-compliance!). Direct costs may include employee and consultant time for assessment, implementation, and monitoring; educating employees about internal control; outlays for new technology to support the internal control program; fees for your independent auditor to perform control testing in order to attest to your assertion regarding the effectiveness of your internal control. Indirect costs may include the reassignment of people and realignment of other resources in the organization to create and maintain a better internal control structure.

However, as stated above, most public companies already have some form of an internal control structure in place. Organizations may not have to buy totally new systems or develop entirely new processes, but instead may be able to tailor their existing resources and integrate them into the new internal control structure.

Step 2
Commit and Organize

Take Stock

Before kicking off your Sarbanes-Oxley internal control project, an informal assessment can help you get your bearings: Understanding how the act applies to your company — based on its business characteristics — can bolster the development of the action plan.

Although virtually all public companies will need to make adjustments before they can confidently evaluate and certify the effectiveness of their internal control, clearly some companies will need to make more sweeping changes than others. To a large extent, the nature of your operations will dictate the scope of changes required. For example, a highly decentralized company may need a more elaborate response to the internal control provisions of Sarbanes-Oxley than a registrant with simpler characteristics.

Company size and complexity presents an interesting paradox. As a rule, implementing internal control in a smaller company is easier since there are fewer people, divisions, processes, etc. to accommodate. Yet smaller companies often have such an informal infrastructure that significant remedial action may be required.

On the other side of the ledger, global companies that must institute control activities at multiple locations may face a significant challenge as they try to reconcile a variety of systems and procedures across the enterprise. In addition, global companies face the challenges of country-specific regulations and unique cultures. These large companies stand to benefit from the uniformity of approach and consistency of application that their internal control program can spur.

Industry — and, more specifically, industry regulations — presents another variable. For example, depository institutions that are subject to the provisions of the Federal Deposit Insurance Corporation Improvement Act of 1991 (FDICIA) have had to abide by internal control reporting rules similar to those in Sarbanes-Oxley for the last 10 years. Yet many depository institutions will need to reinvigorate their programs for assessing the effectiveness of internal control, which, under Sarbanes-Oxley, must now take into account disclosure controls and procedures.

Commit to the Task

With an understanding of how much of an effort your company will likely need to exert, you are ready to begin. We believe this process can only start from one place — the top.

The CEO and CFO should set the tone and initiate the course of action. The board of directors also plays an important role. Although not directly responsible for implementation of Sarbanes-Oxley, the board should

oversee the company's commitment to the task and should be kept apprised of the development of the internal control program.

To serve effectively, the CEO and CFO and the board must, naturally, have a working knowledge of the act. If briefing sessions are required to bring them up to speed, they should be scheduled. Once members have a full appreciation of the demands of Sarbanes-Oxley, the CEO and CFO should formally commit the company to the task and acknowledge responsibility for ensuring compliance.

Next, a formal communication should be made to key management and employees. The communication should include a directive for compliance with the provisions of Sarbanes-Oxley, a definition of the task at hand, general instructions, and the broad assignment of resources.

Form a Steering Committee

We recommend that a steering committee be formed to oversee and coordinate all of your Sarbanes-Oxley activities — including those beyond the scope of Sections 302 and 404 — across the organization. This is a high-level group: Its key members should be knowledgeable about the company's "big picture," be integral to the implementation of company strategy, and have the authority to make critical decisions and allocate resources where and when needed.

In smaller companies, the steering committee may consist only of the two individuals who will be certifying the effectiveness of internal control — the CEO and CFO. In larger organizations, members may include other executives, such as the chief accounting officer, director of internal audit, and general counsel, as well as an advisor from the audit committee. In companies of all sizes, a board of director's designee should be assigned to monitor the steering committee's processes and progress.

Functions of the steering committee will include:

- establishing the parameters under which the disclosure committee will operate;
- identifying the people needed to achieve objectives;
- keeping the board of directors and management informed of progress.

The deliberations and actions of the steering committee — as well as those of any other group working on compliance — should be documented. A written record may lay the roadmap for putting objectives into action. We suggest that you consult with your legal counsel regarding the nature and extent of documentation.

Step 3
Select a Suitable Internal Control Framework

Whether you are starting from scratch or strengthening your existing internal control framework, you should strive for a system that meets four criteria: (1) objectivity, (2) measurability, (3) completeness, and (4) relevance.

Accordingly, many companies build their internal control structure around the recommendations of the Committee of Sponsoring Organizations of the Treadway Commission (COSO). However, COSO represents just one — albeit the most widely recognized — of several internal control frameworks. (See sidebar.)

Internal Control According to COSO

Internal control, as defined by COSO, is a process effected by a company's board of directors, management, and other personnel that drives business success in three categories:

- effectiveness and efficiency of operations;
- reliability of financial reporting;
- compliance with applicable laws and regulations.

Given its ubiquity, COSO will provide the basis of our discussion on selecting a suitable internal control framework. Note that the COSO guidelines, published in 1991, don't explicitly refer to disclosure controls and procedures. Rather, the framework that COSO describes is broader, encompassing both disclosure controls and procedures and internal controls and procedures for financial reporting.

The COSO framework breaks effective internal control into five interrelated components in order to simplify management's task of administering and supervising all of the activities that go into a successful internal control structure.

The Control Environment encompasses every facet of the internal control framework — it is the universe in which all the other elements exist. The control environment includes such concepts as tone, attitude, awareness, competence, and style. It derives much of its strength from the tone established by the company's board and executives.

Frameworks for Internal Control

A number of evaluative frameworks for internal control are available. Among the most prominent are:

A. ***COSO*** - Internal Control-Integrated Framework: Developed by the Committee of Sponsoring Organizations of the Treadway Commission and sponsored by the AICPA, FEI, the IIA, and others, COSO is the dominant framework in the U.S. The guidelines were first published in 1991, with anticipated revisions and updates forthcoming. We believe this will be the framework chosen by the vast majority of U.S.-based public companies.

B. ***CoCo*** - The Control Model: Developed by the Criteria of Control Committee of the Canadian Institute of Chartered Accountants, CoCo focuses on behavioral values rather than control structure and procedures as the fundamental basis for internal control in a company.

C. ***Turnbull Report*** - Internal Control: Guidance for Directors on the Combined Code: Developed by the Committee on Corporate Governance of the Institute of Chartered Accountants in England & Wales, in conjunction with the London Stock Exchange, the guide was published in 1999. Turnbull requires companies to identify, evaluate, and manage their significant risks and to assess the effectiveness of the related internal control system.

D. ***ACC*** - Australian Criteria of Control: Issued in 1998 by the Institute of Internal Auditors – Australia, the ACC emphasizes the competency of management and employees to develop and operate the internal control framework. Self-committed control, which includes such attributes as attitudes, behaviors, and competency, is promoted as the most cost-effective approach to internal control.

E. ***The King Report***: The King Report, released by the King Committee on Corporate Governance in 1994, promotes high standards of corporate governance in South Africa. The King Report goes beyond the usual financial and regulatory aspects of corporate governance by addressing social, ethical, and environmental concerns.

Risk Assessment involves the identification and analysis by management of relevant risks to achieving business objectives. In the course of a risk assessment, each business objective, from highest level (such as "run a profitable company") to the lowest level (such as "safeguard cash") is documented and then every risk that might undermine or block the objective is identified and prioritized.

Control Activities are developed to specifically address each control objective to mitigate the risks identified above. Control activities are the policies, procedures, and practices that are put into place to ensure that business objectives are achieved and risk mitigation strategies are carried out.

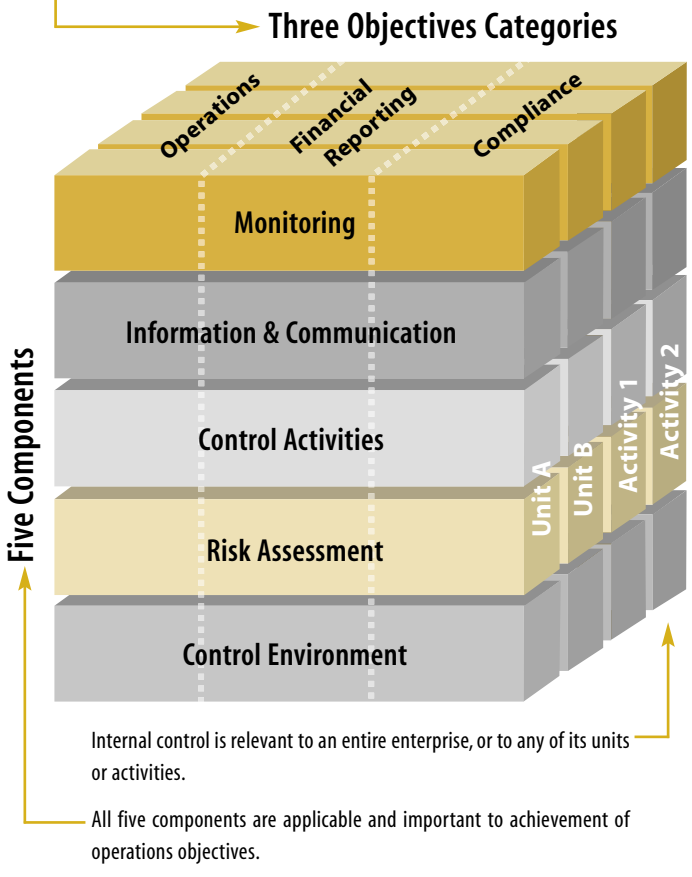
Information and Communication supports internal control by conveying directives from the management level to the employees in a form and a timeframe that allows them to effectively perform their control activities. The process should also work in reverse, communicating information on results, deficiencies and emerging issues from the lowest levels of a company to management and the board of directors.

Monitoring is a process to evaluate and assess the quality of internal control over time through ongoing and special evaluations. Monitoring can include both internal and external oversight of internal control by management, employees, and outside parties.

Relationship of Objectives and Components

There is a direct relationship between objectives, which represent what an entity strives to achieve, and components, which represent what is needed to achieve the objectives.

Information is needed for all three objectives categories—to effectively manage business operations, prepare financial statements reliably, and determine compliance.



Internal control is relevant to an entire enterprise, or to any of its units or activities.

All five components are applicable and important to achievement of operations objectives.

Framework: Mandatory

How important is the internal control framework to your Sarbanes-Oxley internal control program? Consider this:

Without a suitable internal control framework (COSO or similar), full compliance with Section 404 of Sarbanes-Oxley *will likely not be possible*. Remember that under Section 404, your independent auditor must complete a report that attests to your assertion on the effectiveness of your internal controls and procedures for financial reporting. If your company hasn't adopted an internal control framework, *there will be no criteria against which your company or its independent auditor can measure effectiveness.*

Or, to put it another way: You've got to pick the set of rules that you want to play by. And if you don't have any rules, your independent auditor can't referee the game!

Step 4
Empower the Disclosure Committee

The formation and activities of a disclosure committee represent one of the most important controls that a company can implement to ensure that its filings are fair, accurate, timely, and complete.

Indeed, disclosure issues provide much of the impetus behind Sarbanes-Oxley. As noted previously, Section 302 of the act calls for CEOs and CFOs to certify that disclosure controls and procedures are in place and are effective. Additionally, it is possible that the SEC will require a company's independent auditor to attest to the effectiveness of the company's disclosure controls and procedures in addition to internal controls and procedures for financial reporting. In fact, so critical does the SEC deem the issue of disclosure, that the SEC advises all public companies to create a dedicated committee to oversee disclosure activities.

Based on our preliminary observations, effective disclosure committees consist of individuals who:

- are familiar with SEC rules;
- are knowledgeable about the primary aspects of the company's business;
- are familiar with the disclosure practices of peer companies;
- have sufficient stature within the company to initiate action when appropriate.

The size of your company will, in part, determine the makeup of your disclosure committee. Larger companies may have a full complement of personnel with the job titles listed below. Smaller companies may have individuals whose job descriptions span several titles.

Some possible members of the disclosure committee include:

- principal accounting officer or controller;
- general counsel or another senior legal officer responsible for SEC filings who reports to the general counsel;
- principal risk management officer;
- chief investor relations officer;
- chief operations officer;
- general (internal) auditor;
- other officers or employees (including business unit representatives), as the company deems appropriate. Some of these individuals might be heads of key business units, heads of geographic regions, a business development representative, or a human resources representative.

Other parties, such as independent auditors and external legal counsel, can serve as valuable advisors to the disclosure committee, but should not make

Crucial Committees

Initiating or strengthening your internal control program may require a deployment (or redeployment) of personnel. We recommend that several new committees be formed to aid in the process:

Steering Committee: A high level, "big picture" group that oversees and coordinates all internal control activities. In small companies, the steering committee may consist of no more than the CEO and CFO. Larger organizations may have proportionally more members.

Disclosure Committee: The SEC advises all public companies to create a disclosure committee to ensure that company filings are fair, accurate, timely, and complete. The committee sets parameters for disclosure and determines the appropriateness of disclosures in all publicly disseminated information.

Internal Control Program Management Team: Responsible for a large proportion of internal control work. The team's activities may include assessment, development, implementation, and remediation of internal control.

decisions or function as voting members of the group.

The disclosure committee serves numerous functions, including:

- determining appropriateness of disclosures in drafts of all publicly disseminated information;
- overseeing the process by which disclosures are created and reviewed;
- identifying what constitutes a "significant" transaction or event;
- identifying what constitutes a "significant deficiency" and "material weakness" in the design or operation of internal control;
- ensuring that the CEO and CFO are aware of material information that could affect disclosures;
- reviewing control deficiencies with the CEO and CFO to determine whether, individually or in the aggregate, they constitute a material weakness; and making recommendations whether they therefore should be disclosed in the SEC filings.

One of the preliminary acts of the disclosure committee will be to define its mission. To operate effectively, the committee should develop a clear description of its scope of responsibilities. The disclosure committee should seek formal confirmation of its understanding with the CEO and CFO.

The most prominent task facing the disclosure committee will be making sure processes are in place to gather and analyze the information to determine whether proper disclosure has occurred. Among other items, the committee should review:

- all SEC filings, including all 1934 Exchange Act filings (e.g., forms 10-Q, 10-K, and 20-F), and 1933 Securities Act registration statements (e.g., forms S-1 and S-3);
- management's quarterly and annual evaluations of disclosure controls and procedures and internal controls and procedures for financial reporting;
- all press releases providing financial information or guidance, information about material acquisitions or dispositions or other events that are material to the company;
- correspondence broadly disseminated to shareholders;
- all presentations to investor conferences or analysts, in conformity with Regulation FD (Full Disclosure);
- all presentations to rating agencies and lenders;
- internal audit reports;
- briefing books for management;
- briefing books for the board of directors and audit committee;
- the company's disclosure policies for information included on its corporate/investor relations Web sites.

Degrees of Deficiency

When trying to determine whether a control deficiency is "significant," factors such as organization size, the quantitative and qualitative aspects of the risk factors that the activity was intended to mitigate, and complexity of operations need to be taken into account.

Examples of potentially significant deficiencies in the design and implementation of a control activity may include:

- The company has no procedures in place to evaluate the credit-worthiness of new customers.
- The company has no procedures in place to track the value of its equity investments.

(These examples assume that the related business processes and account balances are material to the company at hand.)

Potentially significant deficiencies in the operating effectiveness of control activities may include:

- While the company has procedures in place to evaluate the credit-worthiness of new customers, orders are often processed for accounts that have been blocked.
- Although the company tracks its equity investments, differences between the company's records and third-party statements are not investigated in a timely manner.

Although the disclosure committee is accountable to the CEO and CFO, a member of the disclosure committee may meet periodically with the audit committee to discuss:

- the activities of the disclosure committee;
- the quality of disclosures included in the company's filings;
- disagreements with the CEO and CFO;
- disagreements with external experts such as legal counsel or the independent auditors.

The audit committee can also take a role in resolving significant disagreements. For example, if the disclosure committee recommended disclosure of particular information, but the CEO and/or CFO disagreed, the audit committee could be called upon to influence the final decision.

Step 5
Establish an Internal Control Program

For many companies, complying with the internal control provisions of Sarbanes-Oxley will require significant effort. In fact, the initial work — developing an internal control program and related support infrastructure — may be intensive. However, once the program is well-established, the burden will be eased, and the structure and processes will become part of your company's standard operating procedures.

The following steps, which are explained in detail below, can be followed when establishing an internal control program:

- Plan the Project;
- Assess the Control Environment;
- Define the Scope;
- Build a Controls Repository;
- Perform Initial and Ongoing Tests;
- Monitor.

Plan the Project

We recommend forming an internal control program management team to establish the internal control program. The size and complexity of your company will determine how you allocate personnel resources to the team. In a small company, little organizational structure may be needed; the team may consist solely of part-time members — perhaps a project manager and a few support staff. However, for larger companies, you may need to deploy a significant number of people in dedicated, full-time roles.

For many companies that already have an internal control group, it may not be necessary to form a separate internal control program management team. However, the steering committee should assess whether the existing internal control group has the appropriate personnel to carry out the steps selected by the company.

Once the team is established, a project plan should be created. At a high level, the overall planning process should result in the following:

- understanding and relative agreement on project objectives, deliverables, scope, cost, and approach;
- commitment that the resources needed are available when required;
- agreement on whether outside resources will be used and a description of their role;
- project baseline to which progress can be compared;
- agreement on processes and methodologies used to manage the project.

>Internal Control Reliability Model – The reliability of internal control is often a function of the following characteristics:

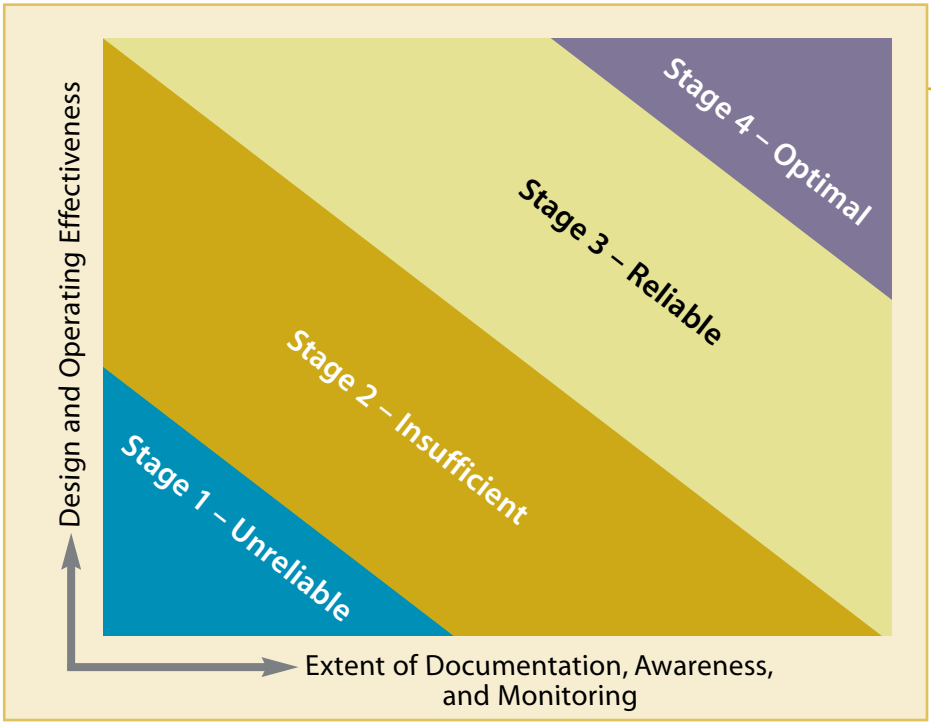
- the design and operating effectiveness of controls;
- the extent of documentation of controls and procedures;
- employee awareness of the control activities that they are responsible for;
- independent monitoring.

In developing a project plan, the internal control project management team may find it helpful to use a tool such as the Internal Control Reliability Model.

The Role of Internal Audit

Many companies already have an internal audit function, and in light of recent proposals by certain stock exchanges, we expect that many more companies will be establishing the function in the future. Internal audit members can play an important role in a company's Sarbanes-Oxley activities by contributing their knowledge of processes and internal control, monitoring management's assessment activities, providing input to a risk assessment process, and serving as an important link to the audit committee.

Internal Control Reliability Model



	Stage 1 – Unreliable	Stage 2 – Insufficient	Stage 3 – Reliable	Stage 4 – Optimal
Characteristics	Controls and related policies and procedures are not in place and documented. A disclosure creation process does not exist. Employees are not aware of their responsibility for control activities. The operating effectiveness of control activities is not evaluated on a regular basis. Control deficiencies are not identified.	Controls and related policies and procedures are in place but not fully documented. A disclosure creation process is in place but not fully documented. Employees may not be aware of their responsibility for control activities. The operating effectiveness of control activities is not adequately evaluated on a regular basis and the process is not fully documented. Control deficiencies may be identified but are not remediated in a timely manner.	Controls and related policies and procedures are in place and adequately documented. A disclosure creation process is in place and adequately documented. Employees are aware of their responsibility for control activities. The operating effectiveness of control activities is evaluated on a periodic basis (e.g., quarterly) and the process is adequetely documented. Control deficiencies are identified and remediated in a timely manner.	Meets all of the characteristics of Stage 3. An enterprise-wide control and risk management program exists such that controls and procedures are documented and continuously reevaluated to reflect major process or organizational changes. A self-assessment process is used to evaluate the design and effectiveness of controls. Technology is leveraged to document processes, control objectives and activities, identify gaps, and evaluate the effectiveness of controls.
Implications	Insufficient documentation to support management's certification and assertion. Level of effort to document, test, and remediate controls is significant.	Insufficient documentation to support management's certification and assertion. Level of effort to document, test, and remediate controls is significant.	Sufficient documentation to support management's certification and assertion. Level of effort to document, test, and remediate controls may be significant depending on the company's circumstances.	Implications of Stage 3. Improved decision-making because of high-quality, timely information. Efficient use of internal resources. Real-time monitoring.

This model, which visually depicts the degree of reliability of internal control, can be applied to any unit for which a plan is being created (e.g., the company as a whole, a single business unit, or a subsidiary). A version of the Internal Control Reliability Model, which is shown on page 21, is designed to categorize the reliability of internal control into four stages: (1) unreliable, (2) insufficient, (3) reliable, and (4) optimal, based on the characteristics listed in the table.

When using the Internal Control Reliability Model, the project team should carefully assess the characteristics of the unit being evaluated and designate the stage that most closely resembles the status of internal control of the unit being evaluated.

If internal control is classified as Unreliable (Stage 1) or Insufficient (Stage 2), it is likely that the internal control structure is not sufficient to support the annual attestation requirements. Under such circumstances, we recommend that the project team begin implementing the project plan immediately. If implementation of the project plan is delayed, the company may not be prepared for its annual report on internal control or the related independent auditor's attestation requirements.

Note that the attainment of Stage 3, which signifies that the company's internal control is adequate, is not the end game. Rather, it is Stage 4 that represents the intent of Sarbanes-Oxley whereby corporate governance is linked to effective control activities.

In addition to providing the project team with useful information that can be used to develop the project plan, the Internal Control Reliability Model can serve several additional purposes, including:

- serving as a common model for discussion between management and the independent auditor regarding the reliability of the company's internal control for purposes of management's evaluation of controls and the independent auditor's attestation;
- providing the board of directors and executive management with a highly visual depiction of the reliability of the company's internal control.

Assess the Control Environment

Written policies and procedures are, of course, important and will play a major role in the effectiveness of your internal control structure. Indeed, much of the success or failure of your internal control program may ride on your written documentation. But also critical are the less-tangible attributes of culture, tone, and attitude, collectively referred to as the "control environment." Contributing to the control environment are such elements as the integrity, ethical values, and competence of your company's people; management's philosophy and operating style; delegation of authority and responsibility; and the attention and direction provided by the board of directors. The control environment forms the foundation for all other components of internal control.

Written policies and procedures are important. But also critical are the less-tangible attributes of culture, tone, and attitude, collectively referred to as the "control environment."

To aid in the understanding of the control environment, we recommend that a cultural assessment be performed. By surveying key management and employees throughout the organization, you can quickly gain an understanding of their attitudes toward the company's commitment to creating an effective control environment. If the results of the cultural assessment suggest that the company does not have a strong control environment, you should take remedial steps, such as the following:

- communicating the importance of internal control;
- reinforcing your code of conduct and ethics and compliance program;
- reestablishing the proper "tone at the top";
- conducting training and awareness programs;
- establishing channels for open communication (including anonymous reporting mechanisms).

Conversely, if the results of the cultural assessment

indicate that the company has a strong control environment, you will have a strong foundation on which to build your internal control program.

Define the Scope

The goal of the scope definition process is to identify and inventory risks related to financial reporting and disclosure. This will allow the internal control program management team to devote their efforts to identifying or designing controls to address such risks. (Note that the focus of this phase of the project — financial reporting and disclosure risks — is more narrow than a full-scale enterprise-wide risk assessment.)

While some companies may already have a formal or informal risk assessment program in place, it should be revisited by the project team to ensure that it encompasses the comprehensive process of identifying all financial and disclosure risks.

> The project team should document and prioritize each financial reporting and disclosure risk.

The project team should begin the scope definition process by identifying all of the company's key business units, locations, and subsidiaries. Next, the team should interview management personnel within these business units to identify financial reporting and disclosure risks that could adversely affect the entity's ability to accurately report financial and non-financial data consistent with following objectives: all amounts and disclosures are accurate, complete, fair and timely.

Management should be prepared to address, among other things, the following during the interview process:

- risks that may prevent the company from achieving its business objectives;
- financial reporting and disclosure risks, considering the following:
  - key business processes and systems, including outsourced applications and processes;
  - non-systematic risks and processes (e.g., journal entries and accounting for contracts);
  - significant accounting standards;
  - SEC and industry regulations;
  - instances of non-compliance with company policies and procedures;
  - matters regarding highly judgmental estimates;
  - significant information systems and technology;
  - situations in which management could override controls.

The project team should then document and prioritize each identified financial reporting and disclosure risk, weighing the relative significance and likelihood of a potential adverse effect without regard to the effectiveness of the company's internal control.

Factors to consider when prioritizing financial reporting and disclosure risks include:

- relative risk to the company;
- materiality to the financial statements;
- likelihood of occurrence.

Over time your company may consider integrating the process of prioritizing financial reporting and disclosure risks into an enterprise-wide risk assessment program that addresses all the elements of the COSO framework.

Build a Controls Repository

The controls repository will serve as a clearinghouse for information and activities related to internal control. It will contain documentation on control objectives, the design and implementation of control activities, as well as methods for testing the operating effectiveness of such activities. It will be the database on which quarterly, and annual management evaluations, as prescribed by Sections 302 and 404, will be based.

To develop this Control Repository, we recommend the following steps:

- define key control objectives;
- map existing control activities against control objectives;
- identify areas where needed controls are absent and remediate.

>Define Key Control Objectives – As a result of the scope definition process, you should have produced an inventory of key financial reporting and disclosure risks. The internal control program management team should systematically work through the risks to define the key control objectives. We recommend that the team focus on risks that have been deemed "high priority" first and work down through the other categories in successive steps, as appropriate for your environment.

A control objective describes what management is seeking to achieve. In the financial reporting area, examples of high-level control objectives include the following:

- Authorization: Transactions are executed in accordance with management's general or specific authorization.
- Recording: All authorized transactions are recorded in the correct amounts, in the correct time period, and in the appropriate account to permit the preparation of financial statements in conformity with generally accepted accounting principles.
- Safeguarding: Responsibility for physical custody of assets is assigned to specific personnel who are independent of related record-keeping functions.
- Reconciliation: Recorded assets are compared with existing assets at reasonable intervals, and appropriate action is taken with respect to any differences.

Examples of "actionable" control objectives include the following:

- Order Management Process: Sales orders are only processed within approved customer credit limits.
- Purchasing Process: Amounts posted to accounts payable represent goods purchased.

>Map Existing Control Activities Against Control Objectives – Control activities are policies and procedures that help the entity to achieve its stated control objectives. Control activities should be embedded within the operations of the business and used to reduce financial reporting and disclosure risks to reasonable levels.

Examples of control activities include the following:

- approvals, authorizations, and verifications;
- direct functional or activity management;
- review of performance indicators;
- security of assets;
- segregation of duties;
- information systems controls.

The objective of this step is to inventory existing control activities practiced within the organization and map those against the comprehensive list of control objectives developed in the previous step.

>Identify Areas Where Needed Controls Are Absent and Remediate – Once all the existing control activities have been mapped to control objectives, it is probable that there will be control objectives for which corresponding control activities do not exist. These gaps should be identified and documented for remediation.

Or, inversely, there may be control activities identified that could not be mapped to an objective. In this context, these could be either unnecessary control activities that could be eliminated or an indication that a needed control objective has not been identified.

All of the gaps noted above should be remediated through a systematic process, starting with high-priority control objectives, until all significant control objectives have control activities to address them.

Perform Initial and Ongoing Tests

Once the controls repository has been developed, the operating effectiveness of the control activities should be evaluated. This evaluation can be performed by the individuals responsible for enacting the controls, or by company management, or by the internal control program management team. The objectives of these initial testing activities are as follows:

- to ensure that control activities are functioning properly;
- to provide information to support further remediation efforts when testing activities reveal internal control deficiencies;
- to develop a sustainable testing program that will support management's quarterly and annual evaluations.

To support the required quarterly and annual evaluation of internal control, an analysis of the internal control structure should be conducted to ensure that no significant changes have occurred since the last evaluation period. If there have been major business process or organizational changes (e.g., an acquisition), it may be necessary to repeat the steps above to modify the internal control structure to address such changes.

The individuals responsible for the control activities should then evaluate their effectiveness as part of a formal internal control self-assessment process. As part of this assessment process, we recommend that the operating effectiveness of the individual control activities be tested and that appropriate documentation be retained so that it can be reviewed by the independent auditors as part of their attestation engagement procedures.

Monitor

For many companies, the internal audit function will play an important role in monitoring and reporting on the effectiveness of the internal control structure. Companies without an internal audit function may consider using the internal control program management team to perform these duties.

Monitoring activities that should take place include the following:

- independent assessment of the adequacy of the data contained in the controls repository;
- verification that testing activities are complete, accurate, and timely;
- confirmation that those who have evaluated control activities have done so in a timely fashion, and with the full and complete understanding of the implication of such a confirmation;
- substantiation that complete and accurate documentation is maintained.

Enabling Technology to Achieve Results

The sheer logistics of compliance with the internal control provisions in Sarbanes-Oxley can seem daunting. Yet the burden can be greatly eased through the strategic use of compliance tools.

Tools can aid in a variety of tasks: designing controls, documenting controls, analyzing and remediating control gaps, improving disclosure, managing risks, documenting review and sign-off, and providing improved management reporting.

Your use of tools is limited only by your needs and your pocketbook. In general, the needs of — and the financial outlay for — smaller companies will be less than that of larger, more complex organizations. But regardless of company size and complexity, the tools and technology that you select should be consistent with the needs of your organization.

> The burden of compliance with the control provisions in Sarbanes-Oxley can be eased through the strategic use of compliance tools.

Tools should not be regarded as an easy solution to a difficult problem. All tools will need some customization to work effectively. Guard, too, against getting seduced by the technology — a proper tool should simplify rather than complicate the process. Finally, keep in mind that tools should augment your personnel, not replace them.

Before you make any capital expenditures on tools, be sure to tailor your existing resources that might support your internal control program. For example, many companies maintain an intranet that could serve as a repository for internal control-related information and documents. Below is a summary of some options.

Databases

Database programs are available to support your internal control program. A controls database can help companies to document their processes, existing control objectives, and activities, and to identify gaps and track actions to remediate those deficiencies. By adding a visualization layer to the controls database, executive management can quickly understand the results of the controls evaluation, which will aid in completing their quarterly certification of controls.

Proprietary Tools

Many professional services firms offer proprietary tools to assist companies in connection with developing an internal control program. Deloitte & Touche, for example, uses the Risk and Controls Knowledgebase™ (RACK), a central repository of industry-specific and controls information, structured according to business process. Using RACK, Deloitte & Touche professionals can quickly tailor process and control information for companies.

Risk and control tracking systems are Web-based self-assessment and monitoring systems designed to support larger and more sophisticated client needs. They are often flexible and scalable tools that help organizations document, monitor, and periodically assess the effectiveness of the internal control structure. These systems are designed to address company needs ranging from initial assessment to risk tracking to support certification, and hence are designed to support multiple phases of the compliance process. Deloitte & Touche has developed the Risk and Control Tracking System (RCTS) to assist companies to structure, manage, and track the assessment process and remediation plans, as well as to aggregate results in a single repository. This structured approach is intended to improve management control and centralized reporting, which should facilitate the disclosure process.

Whatever system you choose to deploy, it may be prudent to run a pilot program on a manageable scale — such as a division, department, or business unit — before rolling out the system across the enterprise.

Conclusion

Compliance with the letter, let alone the spirit, of Sarbanes-Oxley may be a daunting task. But in order to reach a higher level of corporate integrity and performance, compliance with the law in and of itself may be inadequate.

In this regard, certain precedents can help point out pitfalls and highlight best practices. For example, the Federal Deposit Insurance Corporation Improvement Act of 1991 (FDICIA) was to the banking industry what Sarbanes-Oxley is to public companies: Both introduced regulations to remedy perceived market failures, and each enacted significant new reporting requirements. It has been more than 10 years since FDICIA took effect, and even ardent critics would concede that the regulation's main objectives — the prevention of large depository institution failures — have been largely achieved.

There are several lessons public companies can learn from the FDICIA example that will help ensure success at both the individual company level (corporate integrity and responsibility) and overall financial markets level (transparency and symmetry of information).

1 *Accept that the environment has profoundly changed.*

Companies must recognize that they operate in a new environment — one that demands more effort and accountability. If your company fails to develop a comprehensive internal control framework, you will not have adequate documentation to support your quarterly and annual evaluation of internal control and your independent auditor may have trouble delivering the quality work you need in a timely fashion.

2 *Promote understanding of internal control within the organization.*

Recent studies conducted by regulatory agencies showed that in the case of two major banks, executives signed assertions in good faith, yet were not able to demonstrate any control over the assessment process, because they did not understand the full implications of their assertions. In other cases, employees were found to be filling out checklists and quarterly internal control report packages without understanding the purpose behind each document. The point here is that while companies may be tempted to show superficial compliance with Sarbanes-Oxley, such an approach may backfire if controls fail because form was stressed over substance.

3 *Factor into your business model the cost of developing an internal control program*

A number of small banks have had sound business plans, but have nonetheless failed because they did not take into account the (substantial) costs associated with developing an internal control program to comply with the FDICIA regulations. We anticipate the same may be true for public companies subject to Sarbanes-Oxley. Good internal control is not a one-time expense; rather, it fundamentally changes the costs of doing business.

Recent events have placed us in a unique period in the history of American business. The call for corporate responsibility has never been greater. The need to link sound corporate governance to effective control activities has never been clearer. And in terms of restoring public confidence in the financial market, there has never been more at stake. Forward-thinking companies and executives will seize the opportunity. Those who fail to act may pay a heavy price.

Understanding the Limits of Internal Control

While internal control can help to *mitigate* risks, it does not *eliminate* risk altogether. Internal control can only provide reasonable — but not absolute —assurance that a company's objectives are met. Internal control is, after all, built on processes involving people, and, as such, is subject to all the limitations of human involvement.

Internal control can be circumvented deliberately: through fraudulent acts by individuals or collusion between employees. Internal control can be undermined inadvertently: through poor judgment, carelessness, distraction, or other breakdowns of processes and procedures. And internal control may be weakened or even eliminated by resource constraints: the relative costs and benefits of internal control must be continually reevaluated.

Epilogue: Sustaining Momentum

Making the changes you need to comply with Sarbanes-Oxley can help your business earn more and be more successful. But why stop there? Good corporate governance involves many other processes that, even if not mandated by law, can give your business a competitive advantage. So in the interest of maximizing your long-term success, here are some other issues that you may want to address as you re-evaluate your corporate governance procedures.

Establish a Code of Ethics

Good corporate governance begins with the "tone at the top" — the behavior and ethics of a company's leadership team. The Sarbanes-Oxley Act, in fact, recognizes this necessity by proposing that every public company disclose whether it has developed a code of ethics for its principal executives and senior financial officers.

Management is responsible for making sure that everyone in the company, from the CEO on down, both knows the code of ethics and behaves in accordance with it. You can do this in the same way that you establish effective internal control: evangelize, enforce, model, instruct, and infiltrate. Above all, make sure that everyone understands, in concrete terms, what they must do in order to comply with the code. It may be helpful to draw up several illustrations that define appropriate behavior for individuals in different corporate roles so that each employee knows what "ethical behavior" means within his or her own job.

The difficulty with implementing good corporate ethics is not so much in the resolution of issues, as it is in the *identification* of issues in the first place. In today's complex business environment, where there are countless shades of gray but little undiluted black and white, it is nearly impossible to foresee all situations presenting an ethical dilemma. Efforts must focus on helping employees identify these potentially "thorny" situations and encouraging them to seek guidance through established reporting mechanisms.

Formalize Operational and Compliance Controls

Although this publication has discussed a number of controls — financial reporting and disclosure controls being the most prominent — other controls also deserve your attention. We recommend that you take the opportunity, while adjusting your systems and procedures for Sarbanes-Oxley control compliance, to consolidate the management of your operational and compliance controls under the same infrastructure as your disclosure and financial reporting controls. Formalizing similar procedures around your operational and compliance controls will allow you to be that much more confident in your business' ability to avoid unexpected pitfalls and obstacles in these two spheres.

Get Your Audit Committee Involved

Section 301 of Sarbanes-Oxley requires all exchange-listed or NASDAQ-traded public companies to have an audit committee, and many private companies have chosen to establish audit committees as well. Serving on an audit committee is an increasingly challenging job. The members of your audit committee should be individuals who are willing and able to dedicate the necessary time and energy to fulfilling their responsibilities as vigilant overseers on behalf of your company's shareholders. Section 407 of the act also shines a brighter light on whether the audit committee has the requisite financial expertise to protect investor interests. The final rules that implement Section 407 require disclosure of whether at least one member is a financial expert, as defined by the SEC. The names of such members must be disclosed in the annual filing and, if no financial expert is resident on the committee, the company must disclose the reason why. Beyond selecting and supervising the company's independent auditor, the audit committee should review financial reports for completeness and accuracy, and facilitate discussions among management, independent auditors, and internal auditors about issues of quality and integrity.

So invite your audit committee to watch over your internal control implementation and compliance with Sections 302 and 404 of the act. The committee can add real value to the process through objective oversight and seasoned perspective.

Appendix A: Compliance Checklist

✔	Step #	Description	See page #
	1A	Familiarize Yourself with Sarbanes-Oxley Section 302	9
	1B	Familiarize Yourself with Sarbanes-Oxley Section 404	10
	2A	Conduct Informal Assessment of Company Situation	13
	2B	CEO and CFO Commits to the Task of Compliance	13
	2C	Form a Steering Committee	14
	3A	Familiarize Yourself with Internal Control Frameworks	15
	3B	Select Internal Control Framework	15
	4	Form a Disclosure Committee	17
	5A	Establish an Internal Control Program	20
	5B	Plan the Project	20
	5C	Form Internal Control Program Management Team	20
	5D	Assess the Control Environment	22
	5E	Define the Scope	23
	5F	Build a Controls Repository	23
	5G	Define Key Control Objectives	24
	5H	Map Existing Control Activities Against Control Objectives	24
	5I	Identify Control Deficiencies and Remediate	24
	5J	Perform Initial and Ongoing Tests	25
	5K	Monitor	25
	6	Enable Technology to Achieve Results	26

"Moving Forward – A Guide to Sarbanes-Oxley Compliance Through Effective Internal Control" is a publication of Deloitte & Touche's Corporate Governance Services designed to help you clearly understand the fast-evolving requirements of the new regulatory and stock market rules, while keeping your response aligned with your broader corporate goals and strategies. These services focus around four specific areas – board roles and responsibilities, ethics and corporate compliance, risk management and controls, and transparency and disclosure.

For more information, visit us at www.deloitte.com/us/corpgov

About Deloitte & Touche

Deloitte & Touche, one of the nation's leading professional services firms, provides assurance and advisory, tax, and management consulting services through nearly 30,000 people in more than 100 U.S. cities. The firm is dedicated to helping its clients and its people excel. Known as an employer of choice for innovative human resources programs, Deloitte & Touche has been recognized as one of the "100 Best Companies to Work For in America" by *Fortune* magazine for six consecutive years. Deloitte & Touche is the U.S. national practice of Deloitte Touche Tohmatsu. Deloitte Touche Tohmatsu is a Swiss Verein, and each of its national practices is a separate and independent legal entity. For more information, please visit Deloitte & Touche's Web site at www.deloitte.com.

January 2003

Deloitte Touche Tohmatsu