Sarbanes-Oxley Section 404

The Tip of the Compliance Iceberg

Sarbanes-Oxley Section 404

The Tip of the Compliance Iceberg

By Dwayne Jorgensen, CIA, CFE, Director, CTG Sarbanes-Oxley Services Practice

Introduction

Since its passage in 2002, the Sarbanes-Oxley Act has spotlighted the realm of corporate governance as it pertains to compliance with legal regulations. Corporations have spent thousands of hours in preparation for their first attempt to earn an 'unqualified' attestation from their public accountants. That attestation is required to substantiate management assertions as to the overall effectiveness of their internal control frameworks, as mandated by Section 404 of the act.

As the first deadline approaches in December, 2004, many CEOs and CFOs believe they have adequately navigated the course laid out for them by the act. But do corporate efforts to comply with Section 404 supply enough information to avoid the unforeseen complications of future non-compliance events? Or have they addressed only the tip of the compliance iceberg?

Current State

As dramatized in regular headlines, corporate investors are still being unpleasantly surprised by allegations of control breakdowns in flagships of the investment world. Given the nebulous and ramified nature of some transactions, executives are increasingly sensitive to the difficulty of ascertaining whether the proper controls are in place to monitor all related activities effectively. Furthermore, the dynamics of a global economy pose an ongoing challenge to an organization's ability to 'assert' to the overall effectiveness of its control environment. These facts lead to a fundamental question: how can you know your control environment is effective without a full understanding of both the depth of compliance required, and the adequacy of your measurement process?

Letter or Spirit?

Numerous comments by key individuals, including SEC commissioners, have made it clear that the Sarbanes-Oxley Act was not intended as the 'end of all means' as it relates to reassuring the investing public and the federal government about an organization's operations. Rather, the act was intended as a 'means to an end': namely, establishment of an integrated control framework as defined in a landmark report issued by the Committee on Sponsoring Organizations of the Treadway Commission (COSO). By design, that framework would address all aspects of the act as a part of the overall defined corporate governance.

Despite that fact, many organizations have responded narrowly and tactically to Section 404 compliance mandates with 'cascading certifications' that require all layers of management to perform the same certification required of the CEO and CFO on SEC quarterly and annual reports. Many have also adopted a wait-and-see attitude relative to the more far-reaching strategic components of the act, such as disclosure guidelines, whistleblower protocols, and the incorporation of a COSO-based uniform control structure across all the organization's financial and nonfinancial processes.
(Corporate Governance and Independence Monitoring Function, 10/1/2003, CFO Project Volume 2)

Ascertaining the depth of the compliance iceberg must start with management's intention to comply with the spirit rather than the letter of the Sarbanes-Oxley Act. Management must decide whether to establish an adequate and effective control environment based on the internal control framework defined in the COSO report (spirit), or settle for doing only what's required to satisfy individual sections (letter).

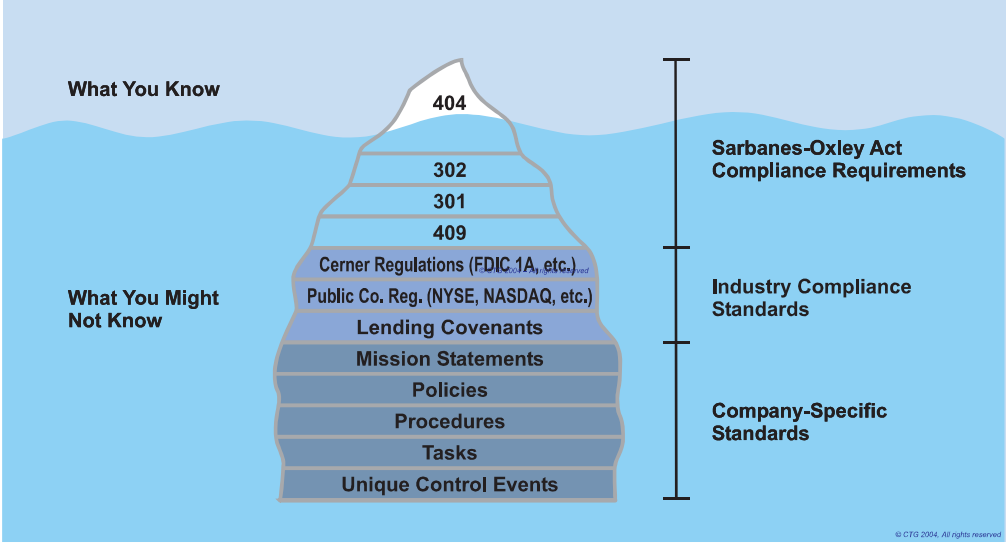

Figure 1: The Compliance Iceberg

As shown in Figure 1, organizations focused exclusively on compliance with Sections 404 and 302 are addressing merely the tip of the iceberg. True adherence to COSO requires adequate measurement of additional layers—other Sarbanes sections, other regulations, lender's covenants, mission statements, policies, procedures, tasks, and unique control events—as part of COSO's ongoing "monitoring process." (See Figure 2 for a description of monitoring in the layers of the 'COSO Cube'.) That means that once management decides to comply with the spirit rather than the letter of the act, it must first determine how much of what has already been done to prepare for compliance with Section 404 can be used for ongoing control measurements.

The Current State of Section 404 Compliance

Since the start of activities to prepare for compliance with Section 404, an ad hoc preparation methodology has emerged. Refined through trial and error, that process has been adopted to various extents by most organizations. It includes these steps:

1. Assess the current state of the organization's controls in key processes.
2. Ensure that the current state is adequate in terms of both the strength and documentation of controls; where they are missing or inadequate, develop them from scratch.
3. Have agencies or individuals independent of the work done in step 2 test the effectiveness of the controls, correct deficiencies where necessary, and then retest.
4. Report the results of the first three steps to prepare for a management assertion letter as prescribed by Section 404, and provide these results to the external auditors for their required attestation of the assertion.

Unfortunately, these four key phases have not been uniformly implemented across all corporations. Cautionary tales abound that relate how organizations have skipped the assessment phase and started at the documentation step, or have authorized the same agencies or people who performed

the work required by step 2 to test it at step 3. In both cases, these inconsistencies have resulted in additional costs for the organization, either in rescoping or in completely redoing the 404 work.

Finally, and more importantly, the work carried out to date in step 4 as the result of this process has not yet been substantiated as the appropriate output, since the final Standards of Testing have not yet been performed by any auditors *(PCAOB Standard #2)*.

How Much Is Enough?

Regardless of the amount of effort already expended on preparing for Section 404, the answer to the fundamental question posed above—how can you know your control environment is effective without a full understanding of the depth of compliance necessary and the adequacy of your measurement process?—may still be "not enough" as it relates to full Sarbanes-Oxley compliance.

Many organizations focused solely on complying with section 404 have contracted with service or software-oriented firms that essentially supplied a 'one-off' product for the 404 report. The significant shortcomings of this approach—which fails to ensure that the outcome will be COSO-compliant as stipulated by the Public Company Accounting Oversight Board (PCAOB) guidance issued to date—will shortly appear in the efforts required to recreate that work for both future annual 404 assertions, and for the quarterly 302 certifications. As shown in Figure 1, COSO compliance extends many levels below the individual sections of the act—all the way down to the individual control activities within the organization. To fully achieve the mandated compliance, an organization must take a more fundamental approach to the elements of the 'COSO Cube.'

COSO: Internal Control—Integrated Framework

The report entitled "Internal Control - Integrated Framework", was commissioned by the Committee on Sponsoring Organizations of the Treadway Commission (COSO). It established a common definition of internal control that meets the needs of various parties not only for assessing their control systems, but also for determining how to improve them.

Figure 2: The impact of Sarbanes-Oxley on the COSO Cube
Source: Internal Control—Integrated Framework, Executive Summary, Committee of Sponsoring Organizations (COSO)

As originally published, the COSO Report was considered a voluntary approach to implementing best practices as they relate to a sound control environment. However, with the passage of the Sarbanes-Oxley Act and the further clarification provided by both the SEC and the PCAOB, the COSO Report has been established as the benchmark for determining compliance with the act. More importantly, as other aspects of the act are more clearly defined or become applicable, the components of the COSO Report take on more meaning. They cover not only the controls necessary for compliance with financial reporting mandates, but also clearly identify the operational controls that will become critical to the accurate assessment and disclosure of all issues subject to disclosure guidelines, whether financial or operational in nature.

The most pertinent aspect of the COSO Report is its establishment, for the first time ever, of a universal definition of internal control:

> *Internal control is broadly defined as 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 control consists of five interrelated components. These are derived from the way management runs a business, and are integrated with the management process. The components are: Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring.*

The following sections provide a brief overview of the nature, significance, and primary drivers of each internal control component named in the report.

Control Environment

The control environment sets the organization's tone, influences the control consciousness of its people, and serves as the disciplinary and structural foundation for all other components of internal control. Key factors in that environment include the integrity, ethical values, and competence of the entity's people; management's philosophy and operating style; the way management assigns authority and responsibility and organizes and develops its people; and the attention and direction provided by the board of directors.

What does this means to an organization? The control environment is the starting point for executive management's decision as to whether compliance with the Sarbanes-Oxley Act will be perceived as a 'spirit' or 'letter of the law' exercise. Organizations that decide to settle for compliance with the letter of the law can reasonably expect to fall short of the expectations of the SEC and PCAOB at some future point, and to reap all the potentially negative consequences of that shortfall. Given that probability, a more prudent approach would be to recognize that while control is management's responsibility, it must be actively embraced by everyone associated with the organization. This tone should be reflected in corporate mission statements; ethics policies; disclosure guidelines; and board, audit committee, and internal audit charters.

Primary drivers of this component include the board of directors, CEO, and CFO.

Risk Assessment

Every entity faces external and internal risks that must be carefully investigated. A precondition to effective risk assessment is establishing objectives that are linked at different levels and internally consistent. Risk assessment identifies and analyzes risks that may affect the achievement of those objectives. It also provides a basis for determining how the risks should be managed. Because economic, industry, regulatory, and operating conditions are all subject to ongoing change, mechanisms are needed to identify and deal with the special risks associated with change.

What this means to an organization is that risk management, formerly the exclusive realm of internal auditors and insurance brokers, is assuming a key management role. In fact, more and more corporations are acknowledging its strategic importance by appointing a chief risk officer (CRO) to give this COSO component the attention it deserves. Ironically, most operational managers confronted by risk assessment policies for the first time are quick to realize how little of their prior responsibilities involved consideration of a 'what-if' component. And yet, as most immediately recognize, only a realistic evaluation of the potential for and impact of a negative outcome can lead to a clear understanding of the steps needed to mitigate that risk.

The ever-changing conditions of the business world make risk assessment a dynamic and ongoing activity. It requires implementing a defined process to guide the organization through the definition of key risk areas, pinpoint specific risks in these areas, evaluate the likelihood and severity of each risk, and identify the resources required to mitigate them to acceptable levels. Now more than ever, the realities of a global business community make the ability to control all significant risks essential to an organization's success.

Primary drivers of this component include the CEO, CFO, CRO, COO; operating management; and the internal auditor.

Control Activities

Control activities are the policies and procedures that embody management directives. They ensure that necessary actions are taken to address risks to achievement of the entity's objectives. Control activities occur throughout the organization, at all levels and in all functions. They are as diverse as approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets, and segregation of duties.

The organizational significance of control activities relates to the fact that most of the effort (and expense) corporations have dedicated to achieving 404 compliance to date has been expended on identifying and documenting these COSO components. Yet, most—if not all—of that effort has been limited to the financial controls as they pertain to the production of the financial statements. As demonstrated in Figure 1, it will be readily apparent to most managers that the next monumental task required by the act will be the inclusion of the other two control areas: business operations and regulatory compliance. The effort required to achieve adequate documentation in these additional areas will depend on the prior state of overall control maturity in the organization.

Primary drivers of this component include the CFO, CRO, COO, and operating management.

Information and Communication

Pertinent information must be identified, captured, and communicated in a form and within a timeframe that enables people to carry out their responsibilities. Information systems produce reports on operational, financial, and compliance-related information that make it possible to run and control the business. They supply not only internally generated data, but also information about external events, activities, and conditions necessary to informed business decision-making and external reporting. Effective communication must also occur in a broader sense, flowing down, across, and up the organization. All personnel must receive a clear message from top management that control responsibilities are to be taken seriously. Workers must understand not only their own role in the internal control system, but how individual activities relate to the work of others. They must have a means of communicating significant information upstream. There also needs to be effective communication with external parties such as customers, suppliers, regulators, and shareholders.

What this means to an organization is that it's not enough merely to document the control activities identified in the 404 compliance exercise. They must be effectively communicated to the rank and file, along with a 'tone at the top' that reinforces the fact that control is everyone's job. In addition, as Section 409 (timeliness of reporting) takes effect, most organizations will be forced to assess yet again the effectiveness of their internal communication systems, with an emphasis on how those systems ensure that information is communicated, processed, and passed along in a timely and efficient manner.

Primary drivers of this component include the CFO and CIO, as well as operating management.

Monitoring

Internal control systems need to be monitored through a process that assesses the quality of each system's performance over time. The process must incorporate ongoing monitoring activities, separate evaluations, or a combination of the two. Ongoing monitoring occurs in the course of operations. It includes regular management and supervisory activities, along with other actions personnel take in performing their duties. The scope and frequency of separate evaluations will depend primarily on an assessment of risks and the effectiveness of ongoing monitoring procedures. Internal control deficiencies should be reported upstream, with serious matters reported to top management and the board.

What this means to an organization is that the most significant success factor in achieving a COSO-compliant control framework is the ability to measure the depth and consistency of compliance with the organization's individual controls. As any internal auditor can testify, three 'steady states' define a typical organization's activities:

- The vision of the executive management team
- The way that vision is translated into corporate policies and procedures
- What is actually done day-to-day by the organization's workers

Generally, these three states—which should be identical—reflect varying degrees of consistency throughout the organization. This inconsistency can typically be tied to the most overlooked and underutilized component of the COSO framework: the monitoring function. More importantly, in an environment still reeling from disclosures of the Enron and WorldCom nature, the separate evaluation mentioned earlier has assumed an increasingly important role in supporting the organization's ability to assure the investing public that it takes the concept of governance seriously. Therefore, as opposed to the static or sporadic monitoring management performed in the past, systems are needed that give management the confidence that real-time monitoring is occurring on all key controls in every process—financial, operational, or regulatory.

Ancient mariners had to rely on manual systems to measure the depth of an iceberg. With the advent of sound navigation ranging, or SONAR, technology was harnessed to provide accurate and real-time measurements. As with the maritime equivalent, technology can significantly improve an organization's ability to measure both the depth and consistency of control compliance. In evaluating the return on investment of technology upgrades, management must compare the costs of the technology against both the costs of the labor required to perform the measurements manually, and the risks associated with inadequate controls that are not continuously assessed on a real-time basis.

Primary drivers of this component include the CEO, CFO, CRO, CIO, and COO; operating management; and internal and external auditors.

Tidal Influences

Some key takeaways already emerging from the various compliance war stories heard to date apply to the areas of planning and the overall control maturity of the organization.

Either of these 'tidal influences' can significantly affect the effectiveness—and the cost-effectiveness—of the organization's measurements of the depth of its compliance efforts. As an example, the effort logged by many organizations to prepare solely for Section 404 compliance has been estimated to exceed 5,000 hours of internal work, with expense estimates ranging from $500,000 to several million. These figures underline the vital importance of ensuring that a methodical approach is taken to determine the depth of compliance necessary for the organization and to realistically assess both the organization's current control maturity and the desired target level once the process is complete.

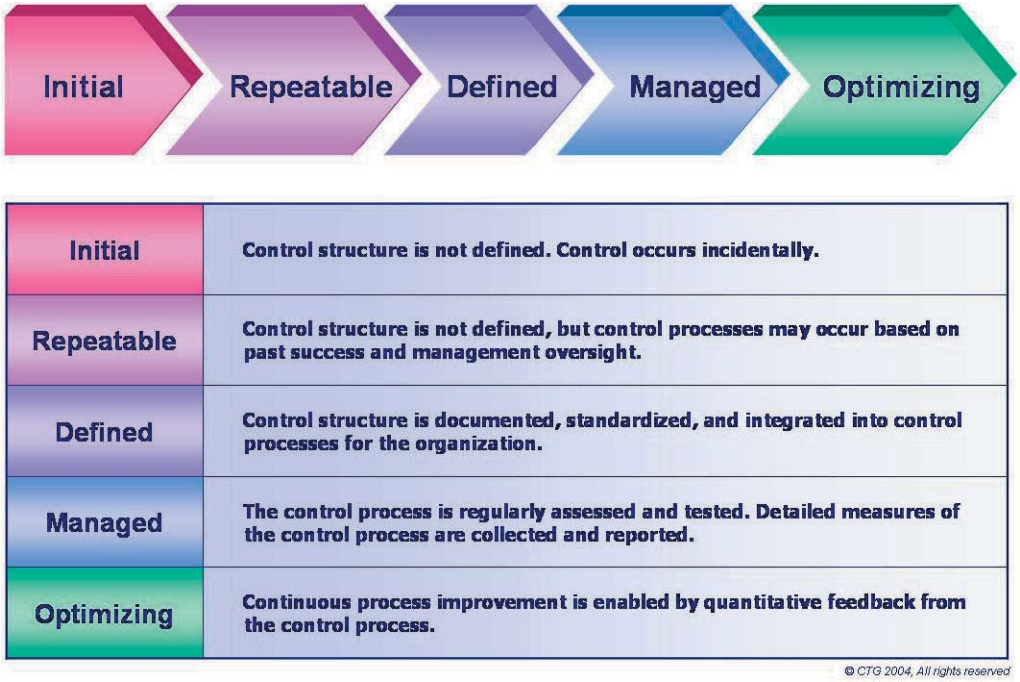

Figure 3: Internal Control Maturity Model

Conclusion

Although many organizations are confident they will meet the Section 404 compliance deadline, that confidence diminishes exponentially when they're asked whether they consider themselves 'COSO-compliant' in relation to all aspects of the organization's compliance iceberg. Most would acknowledge an even lesser degree of confidence that—given the ever-changing nature of the corporate (and regulatory) environment—the work carried out for the first 404 event will equally satisfy future 404 requirements or 302 certifications. That fact poses a second fundamental question: one that all corporate executives should be asking themselves today. "Since 404 compliance is merely the tip of the compliance iceberg, how can I improve my confidence level as regards fully satisfying the need for overall compliance with the spirit (or complete COSO compliance) of the Sarbanes-Oxley Act?"

About the Author: *Dwayne Jorgensen, CIA, CFE (dwayne.jorgensen@ctg.com) is the Director of Sarbanes-Oxley Services for CTG, an international information technology and staffing company. He has served as North American Practice Director of internal audit services for a professional services firm; as a principal of a large consulting firm, where he headed the business process outsourcing practice; and as Director of Internal Audit and Secretary of the Audit Committee for a privately-held hospitality holding company. He is a member of the Institute of Internal Auditors and the Association of Certified Fraud Examiners.*

Computer Task Group, Inc.
Sarbanes-Oxley Act
Automated Continuous Monitoring

Although many organizations are confident they will meet the Sarbanes-Oxley ("SOX") Section 404 compliance deadline, that confidence diminishes exponentially when they're asked whether they consider themselves 'COSO-compliant' in relation to all aspects of the organization's "compliance iceberg." Most would acknowledge an even lesser degree of confidence that—given the ever-changing nature of the corporate (and regulatory) environment—the work carried out for the first 404 event will equally satisfy future 404 requirements or 302 certifications. That fact poses a second fundamental question: one that all corporate executives should be asking themselves today. "Since 404 compliance is merely the tip of the compliance iceberg, how can I improve my confidence level as regards fully satisfying the need for overall compliance with the spirit (or complete COSO compliance) of the Sarbanes-Oxley Act?"

The Sarbanes-Oxley (SOX) service line, along with the Information Security Solutions Practice of CTG, is working with several software vendors to develop an automated software tool to incorporate into its ISO-methodology to address continuous monitoring. At this time, CTG and the vendors are working on a proof-in-concept by integrating this software solution at CTG's world headquarters in Buffalo, NY, where the methodology was already successfully used in CTG's first-ever 404 assertion. The objective of the software tool is to provide companies with a means to effectively and efficiently report on key process and control activities associated with SOX compliance. For key processes associated with financials, the software will:

- Create a complete body of evidence for all phases of assessment, documentation, remediation and attestation with:
    - context searches
    - pre-built reports
    - ad hoc analyses
    - audit walk-through paths
- "Automate" (through work-flow and e-mail protocols) financial controls to strengthen the effectiveness of financial operations
- Overcome organizational and geographical barriers to enforce compliance policies
- Provide scalability as business conditions change and the financial control environment broadens and matures
- Positively impact related monitoring costs, easily producing an "ROI" for the initial investment
- Reduce time-to-compliance with quick implementations and minimal training requirements
- Incorporate changes in the regulatory environment, such as new PCAOB interpretations, and standards pronouncements

For key automated controls associated with the IT infrastructure that supports these key processes, the software will:

- Provide the ability to proactively assess, audit, and secure multi-platform IT environments from internal and external attacks
- Provide scalable patch assessment, packaging and deployment of software patches
- Provide closed-loop identification and resolution to find and eliminate security exposures
- Reduce host- and network-based security breaches using simplified configuration management to manage risks against downtime and revenue loss
- Automate tasks enterprise-wide, enabling organization to be proactive in even the most resource-constrained environments
- Provide auditing capabilities with ready-to-run reports using customization options and audit creation in each environment to improve internal and external results

The software tool will also provide for the deployment of customizable dashboards for continuous tracking and monitoring of key processes and controls, as defined by the users. Dashboards can be created for executive management, internal audit, IT and even external auditors.

The effort logged by many organizations to prepare solely for Section 404 compliance has been estimated to exceed 5,000 hours of internal work, with expense estimates ranging from $500,000 to several million. These figures underline the vital importance of ensuring that a methodical approach is taken to determine the depth of compliance necessary for the organization and to realistically assess both the organization's current control maturity and the desired target level once the process is complete, and to monitor this control maturity on an ongoing basis, with archival abilities to provide artifacts as needed for independent verification. This "continuous monitoring program" under development by CTG and its alliance partners will readily achieve those goals in a cost-effective manner.