The Bulletin

protiviti SM
Independent Risk Consulting

VOLUME 1 ISSUE 6

Internal Controls Over Financial Reporting: Understanding Section 404 of Sarbanes-Oxley

As discussed in Issue 3 of *The Bulletin*, Sections 302 and 906 of the Sarbanes-Oxley Act (SOA) lay a foundation for restoring investor confidence in the integrity of public reporting. Building on that foundation, Section 404 requires management to file an internal control report with the annual report on Form 10-K. This issue of *The Bulletin* addresses in detail Section 404, a provision of SOA that is certain to garner the attention of public company executives in the coming months.

What does Section 404 require?

According to the SEC's proposed rules on Section 404, the annual internal control report must articulate management's responsibilities to establish and maintain adequate internal controls over financial reporting. It must state management's conclusions as to the *design* and *operational effectiveness* of these internal controls at year-end. The report must also state that the company's public accountant has attested to and reported on management's evaluation of internal controls over financial reporting. For most companies, this new attestation requirement will expand the scope of the accounting firm's audit procedures beyond the work required to render an opinion on the financial statements. Finally, Section 404 also requires management to evaluate the effectiveness of its internal controls over financial reporting (as well as the disclosure controls and procedures) on a quarterly basis.

When is Section 404 effective?

The proposed SEC rules make the Section 404 requirements effective for fiscal years ended after September 15, 2003. This time frame will give the Public Company Accounting Oversight Board (PCAOB), the newly established watchdog of the accounting industry, an opportunity to establish the relevant attestation standards. The delay is also intended to provide sufficient time for public companies and their independent auditors to prepare for compliance.

What are internal controls over financial reporting?

The proposed Section 404 rules define internal controls related to financial reporting as "controls that pertain to the preparation of financial statements for external purposes that are fairly presented in conformity with generally accepted accounting principles" as addressed by professional auditing standards. The auditing standards referenced by the proposed rule defines internal controls as a process – effected by an entity's board of directors, management and other personnel – designed to provide reasonable assurance regarding the achievement of three broad objectives: reliability of financial reporting; effectiveness and efficiency of operations; and compliance with applicable laws and regulations. This definition is based on the Internal Controls – Integrated Framework provided by the Committee of Sponsoring Organizations (COSO) of the Treadway Commission.

The Integrated Framework provides guidance for how management should evaluate its internal controls. The most important criterion is whether the internal controls are designed to provide reasonable assurance that a given objective is achieved. While many management teams will desire to address all three COSO objectives, as introduced above, the focus of Section 404 is on financial reporting.

The second criterion required by COSO addresses the focus of the review. Internal controls must be evaluated at two levels: the entity level (the enterprise as a whole) and the process level (where transactions are processed).

Finally, management must consider whether there are five components of internal controls in place – (1) control environment, (2) risk assessment, (3) control activities, (4) information systems and communication, and (5) monitoring – at both the entity level and the process level, and if so, whether the internal controls provide reasonable assurance that the stated objective (e.g., reliability of financial reporting) is met.

Which companies must comply with Section 404?

The requirements to file an internal control report under Section 404 are triggered when companies file quarterly and annual reports with the SEC under either Section 13(a) or 15(d) of the Securities Exchange Act of 1934 (the "Exchange Act"). The requirement is being integrated with current SEC rules and forms for filing these reports.

Who should be involved in complying with Section 404?

One of the certifying officers (i.e., the CEO or CFO) should serve as the project sponsor. Management should organize a project team consisting of (1) a project leader (the corporate controller or chief accounting officer, for example); (2) operating, accounting and auditing representatives from the company's major business units, including its foreign operations; (3) corporate executives such as the chief information officer and chief audit executive; (4) appropriate subject matter experts (e.g., experts in IT, derivatives,

reserve estimation and other areas requiring specialized knowledge); and (5) others needed to make key decisions. This team should interface with independent advisors and legal counsel whenever there is a need for input. This project team is a separate group from the disclosure committee (see Issue 3 of *The Bulletin*).

If internal resources are not available and a substantial amount of work is required, it may be advisable to arrange for assistance from an independent outside party. If the project requires a significant amount of work to complete, management should establish a project management office, supported by a dedicated core of full-time staff.

What's the value proposition?

The reduction of regulatory risk (i.e., the risk of noncompliance with SOA and the SEC's regulations) is accomplished through well-documented and monitored processes and controls that provide a credible body of evidence that management has established effective internal controls over financial reporting. A process-based approach sources the risk of significant errors and omissions within the processes, and identifies key control points. This approach enables management to better manage the critical processes and drive accountability throughout the organization.

A controls assessment provides benefits beyond regulatory compliance. For example, management can have its processes and procedures periodically and systematically confirmed by control owners in order to reinforce accountability and further reduce the risk of financial reporting restatements and fraud, which can severely impact market capitalization and reputation. Management can also broaden the focus of the controls assessment to identify improvements in process effectiveness and efficiency in order to reduce costs, e.g., reduce closing process cycle time, simplify and eliminate redundant and inefficient controls, improve effectiveness of controls design, and reduce the level of increased external audit fees. Finally, management can focus the assessment of processes to better manage the business, e.g., satisfy customers faster, better and at lower cost.

How are internal controls over financial reporting related to disclosure controls and procedures?

The SEC introduced "disclosure controls and procedures" as a new term in its August 29, 2002, release providing rules pursuant to Section 302 of SOA. Disclosure controls and procedures are designed to ensure that all material information is accumulated and summarized for timely assessment and disclosure pursuant to the SEC's rules and regulations. The SEC intended to make it explicit that the controls contemplated by SOA should embody controls and procedures addressing the quality and timeliness of financial and nonfinancial disclosure in public reports.

Internal controls over financial reporting are a subset of disclosure controls and procedures. In its proposed rules on Section 404, the SEC states, "... in large part, we believe there is significant overlap between these two types of controls and procedures."

In plain English, what has to be done to comply?

For many companies, Section 404 compliance is a major project. Accordingly, companies should organize to do the following:

- **Select the priority financial reporting elements.** Select the priority accounts and disclosure items considering the significance to financial reporting and the risk of misstatement.
- **Conduct entity-level assessment.** Often referred to as "tone at the top," entity-level controls are much more than that. They include ethics programs, entity-level monitoring activity, risk identification processes, investigation protocols, audit committee communication protocols, IT infrastructure controls, etc.
- **Document the processes.** Document the transaction flows that materially impact the priority financial reporting elements.
- **Source the risks.** Determine what can go wrong within the processes that could result in errors or omissions.
- **Document the controls.** Document the internal controls at the source of the risk (preventive controls) or downstream in the process (detective controls). Identify who owns the controls.
- **Assess controls design.** Assess the effectiveness of controls design in reducing to an acceptable level the risk of errors or omissions.
- **Validate the operation of controls.** Test the controls to verify they are performing as designed.
- **Report.** When the assessment is complete, management should conclude as to the effectiveness of the internal controls over financial reporting, communicate its conclusions to the external auditors and audit committee, and issue the internal control report.

Section 404 is not entirely new

Large banks began complying with the Federal Deposit Insurance Corporation Improvement Act of 1991 (FDICIA), developing innovative approaches for compliance. While there are some differences, there are many parallels between FDICIA and Section 404 of SOA, including similar requirements, goals and frameworks.

What lessons can we learn from the banks that have been down this road? First, it is never too early to begin. Second, apply a comprehensive framework, such as COSO, to provide a consistent approach. Third, involve the external auditor early and at frequent checkpoints during the process to understand the key judgments made by management. Fourth, make sure your risk assessment is comprehensive.

The initial annual assessment is only the beginning

The key controls identified during the initial annual assessment provide the basis for conducting quarterly evaluations going forward. Here is the ideal sequence of events:

- The initial annual assessment documents the key controls by process and by owner or responsible party.
- Management issues the internal control report. The external auditor reports on management's internal control assertions on an annual basis.

- On a quarterly basis, process owners self-assess the effectiveness of the controls for which they are responsible. Customized questions are developed for use in the self-assessment process based upon input of key controls identified during the initial annual assessment.

- Process owners report to unit managers at or sufficiently close to the end of each quarter. Unit managers, in turn, report to top management (the certifying officers) or to the disclosure committee. Any exceptions are reported to the officer designated with the responsibility to resolve them. Web-based technology may be useful in facilitating this upward reporting process.

- With process-owner feedback, management will be positioned to focus on change, e.g., change in processes, systems, operations and other factors, and its potential impact on the overall control structure.

- Management issues its certification on internal controls over financial reporting on a quarterly basis in the years following the initial annual assessment.

Because the initial annual assessment is process-based, the upward reporting by process owners will truly be a "chain of accountability," which will contrast with the "chain of certifications" created by many companies that require their direct reports to certify results individually. In practice, those direct reports have, in turn, often required the same of their direct reports, and so on down the chain of command. The chain of certifications approach may engage process owners, but it does not necessarily provide assurance that better information will be furnished to management for timely action and disclosure. The chain of accountability arising from the linkage of the results of the initial annual assessment to the ongoing quarterly evaluations results from a process-based approach.

Should management engage the independent public accountant to create original documentation of its internal controls?

The safe answer in today's environment is probably not. According to Rule 2.01 of Regulation S-X of the SEC, the external auditor must be independent both in fact and in appearance. While the standards have not been promulgated by which the external auditor will be required to attest, significant involvement in the documentation of a company's internal control structure, followed by an attestation process in which the same documentation is reviewed, would be tantamount to keeping the books and auditing the books. The SEC's position is that the auditor cannot audit his or her own work.

One practical approach to addressing this issue is to focus on the magnitude of the documentation required to bring a company into compliance. This approach, which has been embraced by one major accounting firm, would prescribe that any situation in which "significant" documentation was necessary should avoid engagement of the external auditor in other than an advisory role. On the other hand, those environments in which minimal additional documentation was necessary might utilize the external auditor to help management identify and finalize the Section 404 documentation.

Sarbanes-Oxley requires management to establish and maintain controls and procedures to ensure all material information is presented to the public in accordance with the SEC's rules and forms, i.e., management is required to design the internal control structure. The documentation issue represents a minefield for boards and management teams because it will forever remain difficult to delineate the difference between documenting the internal control structure and designing the internal control structure. Documenting an internal control structure is similar to "blazing a trail." It requires a decision-tree type approach in which someone must decide each path to achieve an appropriate control structure. The selection of the primary path is a function of the risks that management perceives the company faces. Subsequent decision points will revolve around questions such as:

- What is the proper combination of preventive controls or detective controls?

- Does transaction volume and velocity permit manual controls or must computerized system controls be utilized?

- Within a process, how much segregation of duties is required?

- Are there pervasive controls affecting multiple processes and, if so, what is their impact?

- What is the impact of a centralized versus decentralized organization?

These and other decisions require significant professional judgment. They represent trail markers about which management must make the ultimate determination. If the independent public accountant is asked to blaze and mark the trail and subsequently also determine if the markings are correct, then management, the board and the auditor could be exposed to allegations that independence was impaired. While independence in fact may have been preserved, the appearance of independence would be difficult if not impossible to explain in the public arena. If explanations are subsequently required, the accounting firm could be placed in the position of an advocate for management, a position the SEC rules do not permit. Given today's hypersensitive environment, this issue does not appear to be one in which it is in anyone's interest to test.

Other matters for management to consider

In complying with Section 404, there are many additional issues for management to take into account. Following are just some of the many areas to consider:

- **Define your objectives and scope.** Start by understanding the expectations of key constituencies, e.g., the project sponsor, executive management, the disclosure committee and the audit committee. Address key scope issues. For example, which financial reporting elements (i.e., the financial statement accounts and disclosures) should the project team review? How much documentation is enough? How much validation and testing is needed? The scoping considerations should also include the approach at the entity level and at the process level, the locations at which to conduct assessments, and the IT systems to consider. Management must set the criteria for addressing these scoping issues.

- **Establish a plan and define your checkpoints.** Define key activities needed to accomplish project objectives. Develop a detailed work plan including project activities and tasks, sequencing, and timeline. Define critical project milestones and assign appropriate checkpoints along the project timeline

by which to gauge project progress. Identify the responsible parties for checkpoints, e.g., project sponsor, executive management, the audit committee and the external auditor. Use the checkpoints for obtaining review and sign-off, and for obtaining concurrence from those parties.

- **Get in synch with your independent accountant.** Timetables are important, but timing is also of the essence. A best practice is for management to complete the controls documentation and evaluation *at least* by the end of the third quarter of the company's fiscal year so the external auditor can test it and corrective actions (if any are required) can be taken before the point-in-time certification and attestation reports are finalized. There is also the issue of public companies across corporate America having to comply with these requirements. If every company waits until the last minute, there likely will not be enough qualified personnel to complete the necessary work.

- **Define your key success factors.** Define key performance indicators and critical success factors, and incorporate them into the project plan. Obtain agreement from the project sponsor and executive management. Examples of performance indicators include fulfillment of executive management expectations, completion of designated milestones, completion of work at designated locations, participation of unit managers, participation of process owners, completion of the internal audit plan relating to financial reporting controls, and minimal rework of documentation.

- **Inventory what already exists.** Controls documentation may already exist. If so, it should be used. Gather such things as relevant policy and procedure manuals, job descriptions, process-owner documentation, internal audit working papers and reports, prior years' external audit documentation, and documentation of the disclosure controls and procedures supporting the existing certification process.

- **Determine internal resources and external advisors.** Identify internal resources and capacity for completing the project in accordance with the plan. Owners of the critical processes impacting financial reporting should be involved as much as possible in the project planning, documentation, assessment and ongoing monitoring. If internal capacity is insufficient, identify key external advisors and define clear expectations of their contributions to the success of the project and beyond.

- **Don't forget to communicate.** The project team should work with the project sponsor to develop a communications plan. This plan should outline how the sponsor and the team communicate with management, the audit committee and the external auditors through the duration of the project. When designing and implementing a plan, keep in mind that the objective is to build stakeholder commitment by articulating the purpose and importance of the project, the sponsorship of the project, and the project timing and approach to everyone who is primarily responsible for the critical internal controls.

Summary

Most companies already have strong internal controls over financial reporting in place. While a Section 404 compliance project formally documents these controls, it should do more. If investors want transparency in public reporting, management should insist upon a disclosure infrastructure that is organized, intuitive, "in control" and process-based. ■

Key Questions to Ask

Key questions for board members:

- Are management and the independent auditor prepared for the Section 404 requirement? Is it being planned for orderly work over the year to make it more effective, less disruptive and less costly? How is the project being scoped to ensure the review focuses on what matters?
- How is management planning to consider the implications of IT in the controls assessment?
- What is the impact on the cost of the audit? Assuming an audit firm quotes 20 to 30 percent of the annual audit fee, does that mean it will take 20 to 30 percent of the time the annual audit takes? If not, how much of this fee is a premium for assumption of risk?
- If the independent public accountant had to make this certification for the 2002 financials, is there anything that would prevent them – given what they know now – from reporting on the company's internal controls?
- Is the audit committee satisfied that the role planned for the independent accountant during the controls assessment is appropriate?

Key questions for management:

- Is there a detailed project plan with clearly articulated responsibilities, milestones, checkpoints and key success factors? Is management planning to complete the controls documentation and evaluation *at least* by the end of the third quarter of the company's fiscal year?
- Are there effective communications with the independent auditor?
- Has the level of outside assistance necessary been determined, based on resource availability and skills needed? For example, is assistance needed with respect to process and controls documentation, project management and guidance, assessment technology and support, and development of customized assessment questions?
- Do project communications articulate clearly what is expected of process owners now, what is expected of them during the project and what is expected after completion of the project?