TESTIMONY OF

GRACE L. HINCHMAN

SENIOR VICE PRESIDENT

FINANCIAL EXECUTIVES INTERNATIONAL

BEFORE THE

U.S. HOUSE OF REPRESENTATIVES

GOVERNMENT REFORM SUBCOMMITTEE on REGULATORY AFFAIRS of THE COMMITTEE ON GOVERNMENT REFORM

AT A HEARING ON

THE SECURITIES AND EXCHANGE COMMISSION'S IMPLEMENTATION OF THE SARBANES-OXLEY ACT, WITH PARTICULAR ATTENTION ON THE REQUIREMENTS OF SECTION 404

APRIL 5, 2006

Thank you Chairman Miller, Ranking Member Lynch and Members of the Subcommittee for this opportunity to appear before you today. I have prepared remarks, I would respectfully request that the full text of my testimony and all supporting materials be entered into the public record.

My name is Grace Hinchman and I am the Senior Vice President of Financial Executives International (FEI). FEI is the leading organization of 15,000 members including CFOs, Treasurers, Controllers, and other senior financial executives. I am pleased to have the opportunity to share the views of our members with you today on the important issue of the SEC's implementation of the Sarbanes-Oxley Act and in particular Section 404 of the Act, which addresses internal control over financial reporting.

STRENGTHENING CORPORATE GOVERANCE, INTERNAL CONTROLS

First, FEI strongly supports the goals of the Sarbanes-Oxley Act, as it has enhanced the role of corporate financial executives and created a greater appreciation for their role within the corporate environment and among the public generally. Specifically, Section 404 of the Act has also strengthened the ability of financial executives to institute continuous improvements in internal controls and financial reporting and to gain enhanced "buy-in" by all employees of the need for strong internal controls. The Act has resulted in the following positive developments:

- Strengthening the tone at the top by requiring certifications of financial statements by CEOs and CFOs, and by requiring management and auditors' reports on internal controls over financial reporting;
- Strengthening the incentives for high quality financial reporting that can be relied upon by the public, by increasing penalties for doing otherwise, including, importantly, the

federal sentencing guidelines for criminal conduct in connection with fraudulent financial reporting;

- Strengthening the requirements for audit committees, which play such a critical role in corporate governance on behalf of the investing public;
- Making the internal control process more rigorous, and heightening accountability; and
- Limiting transactions such as loans to officers, which is part and parcel of good corporate governance.

Even before Sarbanes – Oxley, internal controls were a long established management tool used to detect and correct deficiencies. Companies have long had what are referred to as “management letters” from their auditors in which certain internal control weaknesses are noted in addition to reports of their own internal audit staff. The Sarbanes-Oxley Act has added gravitas to the impact of any reports of substantive internal control weaknesses and the need to correct them by raising the bar of public disclosure of material weaknesses. Today, public companies, both large and small, must show that their system of internal control over financial reporting is effective and without material weaknesses. This focus on strength and effectiveness in a company’s system of internal controls should enhance a shareholders faith in the integrity of a company’s financial reporting data. FEI believes it is critical, that in order for Section 404 of Sarbanes-Oxley to be most effective, requirements of a management assessment and supporting attestation on internal controls must be integrated with management’s and auditor’s efforts surrounding the presentation and audit of a company’s financial reporting.

Overall, FEI believes that the heightened emphasis on internal controls, corporate governance and the enhanced role of financial executives brought about by Sarbanes – Oxley have all been very positive.

IMPLEMENTING THE SARBANES-OXLEY ACT OF 2002

While many of the mandates of the Sarbanes-Oxley Act were effective upon the adoption of the legislation, much of the Act directed the SEC and PCAOB to develop the “rules” of implementation of the Act. Generally, the SEC and the PCAOB have done an impressive job in fulfilling a difficult task by striking a balance in efficiency and cost effectiveness while maintaining the integrity and intent of the statute. However, the rules and standards related to the implementation of Section 404 of the Act still require significant attention.

I would be amiss if I did not acknowledge the SEC’s recognition of the additional “regulatory overload” its proposal to accelerate the 10-K and 10-Q filing deadlines presented to publicly held companies especially in light of the new Sarbanes – Oxley compliance requirements. Moreover, the Commission has remained mindful of this “regulatory overload” by remaining flexible and demonstrating a willingness to postpone the final implementation of the accelerated filing deadlines and allow companies to devote resources to Section 404 implementation.

FOCUS ON INTERNAL CONTROLS

Over the past few years, FEI has been especially active in working with its members to provide assistance for effective and efficient implementation of the Act generally and Section 404 specifically including the PCAOB’s Auditing Standard No. 2, (AS2) *Audit of Internal Control over Financial Reporting Performed in Conjunction with an Audit of Financial Statements*.

FEI's Committee on Corporate Reporting (CCR) has held two sessions with Section 404 project leaders from many of the Fortune 100 companies to share practices for implementation, and to identify efficiencies as well as areas for improvement. These sessions and their outcomes were documented in two reports by FEI's Research Foundation (FERF) in May and November 2005, which I have included in my written testimony.

FEI's President and CEO, Colleen Cunningham, as well as members of CCR, participated on the SEC's and the PCAOB's Roundtable on Internal Control Reporting in April 2005. We look forward to participating again at the next Roundtable scheduled for May 10, 2006. We believe that these Roundtables are critical to successfully implementing and sustaining the process surrounding Section 404 for preparers and auditors alike. We applaud the SEC and the PCAOB for organizing these sessions.

Additionally, several of FEI's technical and policy committees have filed numerous comment letters on Section 404 implementation issues but we consistently acknowledge that the SEC and the PCAOB are working diligently to achieve an effective and efficient process for Section 404. There are continuing concerns by many FEI members about particular issues that are becoming increasingly evident especially regarding the overall cost of compliance and the ability for many companies to sustain their ability to meet these regulatory requirements.

Although, the SEC maintains final authority over the rules and standards to implement the requirements of Section 404, much of the rule-making and standards setting has come from the PCAOB's AS2. Since the SEC's approval of AS2 on June 17, 2004, the PCAOB and the SEC have continued to release additional guidance to supplement AS2 through policy statements and detailed Staff Q&As. While we believe this additional guidance has been helpful to both preparers and auditors alike, they have fallen short of providing a completely effective and efficient implementation process.

In May 2005, as a result of the feedback received at their April 2005 Roundtable, the SEC and the PCAOB issued additional guidance intended to create greater efficiencies in implementing Year Two of Section 404. FEI continues to support the key tenets of the May 2005 SEC and PCAOB guidance but we believe that additional focus and attention is needed on some of the most critically important tenets:

- The need for integration of the audit of internal controls with the audit of a company's financial statements;
- The need to use a top-down, risk based approach to implementation;
- The need to exercise flexibility and use of judgment in using the work of others.

FEI firmly believes that Section 404 of Sarbanes-Oxley is workable and does not require Congressional action. Instead, the SEC and the PCAOB need to take a reasoned approach to sustaining implementation and to focus auditors and companies more on embracing the key tenets of the SEC and PCAOB guidance versus drowning in the minutia of detailed documentation.

SMALLER COMPANY CONCERNS

The SEC should be commended for its work in establishing the Advisory Committee on Smaller Public Companies (ACSPC) to review and consider the regulatory issues affecting smaller public companies especially the impact of Sarbanes-Oxley compliance. FEI recognizes the concerns with the significant and even disproportionate economic impact the Sarbanes-Oxley Act continues to have on smaller companies.

Smaller companies simply do not have the resources found in the larger companies to sustain the financial and personnel requirements of Sarbanes-Oxley. Smaller public companies are anxious about the high cost of implementing the Sarbanes-Oxley provisions, especially the 404 provisions. FEI believes that some relief is warranted, especially to the micro cap companies. If something does not change, FEI is concerned that many micro cap companies may be driven into extinction in their efforts to comply with the Sarbanes-Oxley requirements. FEI's Small Public Company Task Force (SPCTF), recently filed comments regarding the SEC's ACSPC's recommendations. A copy of FEI's SPCTF comment letter is attached. The SPCTF recommends that further study and guidance is needed to address the core issue of improving the cost-benefit equation of complying with Section 404.

Both the SEC and the PCAOB have the authority today to tailor compliance of Section 404 so it meets the capabilities of all public companies large and small. Such guidance should come in the form of "right-sizing" AS2 in a separate standard directed at smaller public companies in particular, or through "right-sizing" AS2 to address the needs of small and large companies alike. The "right-sized" standard can reflect learnings of the SEC ACSPC as well as information provided at the upcoming May SEC-PCAOB roundtable. FEI remains convinced that the regulatory and standards setting processes possess adequate authority and flexibility to address the Section 404 implementation challenges.

In addition, consideration should be given as to whether the SEC needs to issue further guidance for management, and smaller public company management in particular. As has been widely noted, the SEC's management reporting rule under Section 404 provided sparse guidance for management, and AS2 became the de facto guidance. Although the Committee Of Sponsoring Organizations (COSO) is developing guidance for smaller public companies, it is not yet final and it is unclear whether such guidance will be helpful to smaller public companies in its final form. As one of the sponsoring organizations for COSO, FEI does not support elevating COSO to a standard-setting role.

COST- BENEFIT OF IMPLEMENTATION

I would be remiss if I do not focus a portion of my remarks on the overall cost-benefit of the Sarbanes-Oxley Act. We appreciate the SEC's and PCAOB's acknowledgment that cost of implementation is high. The degree of testing and documentation of internal controls forms the largest part of the cost, and incorporates the need to pay internal staff, both finance and internal audit, as well as the external auditor, and other external experts such as software consultants, to enhance systems related to testing, documenting, and reporting on internal controls. We especially note the significant cost impact on smaller public companies, as they simply do not have the resources to carry out the reporting requirements. The benefit side of the equation, while it includes the strengthening of the role of the financial reporting and internal control process, increased shareholder confidence is still much more difficult to measure and quantify. While FEI certainly supports such intangible benefits, we believe that good corporate governance encompasses not only strong internal controls, but also an eye toward budget, profitability, and as such, cost-benefit issues.

FEI continues to urge regulators to maintain flexibility and judgment that would promote efficiencies rather than redundancies, and minimize extraneous, labor-intensive procedures that are time consuming and expensive. While we do believe that greater efficiencies have been witnessed in year two of implementing Section 404, FEI remains hopeful that more reasonable approaches will continue to be developed that will further reduce the cost of compliance as regulators, preparers, and auditors work together to implement the spirit of the SEC rules and

PCAOB standards. It is our hope that reasonableness will prevail, particularly in the roll forward of continuous testing and documentation in future years.

FEI's COST SURVEY on IMPLEMENTING SECTION 404

FEI has been surveying its membership on Section 404 Implementation costs since May 2003. In March 2006, FEI surveyed 274 public companies, with average revenues of $5.7 billion, (the range being under $25 million to over $25 billion in revenues) to gauge Section 404 compliance cost estimates. Of the 274 respondents, 193 were second year filers, 56 were first year filers, and 25 had not yet filed their results. The survey results showed:

- The total cost of compliance with Sarbanes-Oxley Section 404 is now estimated at $3.70 million for the average company.
- Total cost is a function of internal costs such as internal audit, external costs other than the auditor (such as external consultants and software packages) and audit fees attributable specifically to the Section 404 internal control attestation.
- According to the survey, the average company expended $1.06 million in internal costs (a decrease of 12.2% for second year filers from their first year of implementation), $1.26 million in external costs (a decrease of 21.7%) and $1.38 million in auditor fees (a decrease of 12.7%).
- In total, companies indicated that audit attestation fees represent 44.2% of their total annual audit fees.
- In looking at the implementation cost based on a company's market capitalization, on average, a microcap company with market capitalization less than $128.2 million had total costs of $1.19 million, a small cap company with market capitalization between

$128.2 and $787.1 million had total costs of $1.29 million and a large public company with a market capitalization greater than $787.1 million had $5.33 million in total costs.

Based on the data obtained, it appears that even in its second year of implementation, while companies have experienced some reduction in costs, most significantly in the area of external costs other than the auditor, the cost of Sarbanes-Oxley Section 404 compliance remains high, and continues to be disproportionate to the burdens associated with annual compliance.

WORKING TOWARDS A SOLUTION

In conclusion, FEI supports the efforts of the SEC and the PCAOB in implementing the requirements of the Sarbanes-Oxley Act of 2002 However, it is evident that more work needs to be done in implementing Section 404 of the Act. We are confident that the SEC and PCAOB are up to the task and they possess the authority to do so. Through continuous study, review and feedback from large company and small company preparers, auditors, regulators and investors by the SEC and the PCAOB, FEI is confident that a reasoned approach to Section 404 implementation that is “right-sized” for all public companies will be achieved.

That concludes my remarks. I want to thank the Chairman and members of the Subcommittee for inviting me to participate in today’s hearing.

ferf

financial executives research foundation

Sarbanes-Oxley Section 404 Compliance: From Project to Sustainability

Financial Executives Research Foundation (FERF)
would like to acknowledge and thank
FEI New York City Chapter for graciously
underwriting the printing costs of this
Executive Report.

ferf
financial executives
research foundation

the source for financial solutions

200 Campus Drive
P.O. Box 674
Florham Park, New Jersey 07932-0674
www.ferf.org

an affiliate of financial executives international

Sarbanes-Oxley Section 404 Compliance

From Project to Sustainability

William M. Sinnett
Director of Research
Financial Executives Research Foundation, Inc.

Dr. Robert A. Howell
Distinguished Visiting Professor of Business Administration
Tuck School of Business at Dartmouth

Sarbanes-Oxley Section 404 Compliance

From Project to Sustainability

TABLE OF CONTENTS

Sarbanes-Oxley Section 404 Compliance

From Project to Sustainability

Purpose

Although many aspects of the Sarbanes-Oxley Act of 2002 ("the Act") directly affect financial executives, members of Financial Executives International report that none have caused more additional effort and costs than Section 404 ("Section 404" or "404").

Section 404 requires management of public companies to include in their annual reports an assessment of the effectiveness of their internal controls over financial reporting. Compliance with Section 404 includes management's assessment of its controls, management's assertion whether these controls are effective, and an audit of these internal controls by the external auditor in conjunction with the audit of the financial statements.

While the effort to comply with Section 404 has provided some valuable insights, the time, redeployment of people, and other costs associated with the implementation in 2004 are generally viewed by members of Financial Executives International's (FEI's) Committee on Corporate Reporting (CCR) as not sustainable. Many financial executives from CCR member companies believe that evaluating the results and understanding leading practices of first-year implementation activities is an important step to the long-term sustainability of the Section 404 compliance process.

This report summarizes the compliance practices of leading companies during 2004, and it describes how they are improving their processes in the second year of compliance as they strive toward long-term sustainability. It is based on the experiences of the companies that participate on CCR.

Executive Summary

Based on their companies' experiences in complying with Section 404 of the Act, participants at a special CCR meeting identified and discussed the following compliance process improvements:

Key Controls

- Identify lower risk areas where reliance on the testing of company level controls is sufficient;
- Critically assess the necessary number of transaction-processing controls;
- Take some lower risk accounts out of scope;

- Reduce the number of testing locations with the use of shared service centers;
- Increase the number of and reliance on automated controls versus manual controls; and
- Find a balance between effective internal control and the number of key controls.

Risk Assessment

- Drive audit activity to the highest possible level in the organization;
- Take a top-down approach to risk and planning;
- Use risk assessment to help prioritize businesses and locations to get appropriate coverage;
- Integrate risk assessment with existing enterprise risk management (ERM) initiatives;
- Use shared service centers; and
- Consider the potential for fraud in assessing risk.

Segregation of Duties

- Ensure that all areas that represent key controls have established and sustainable segregation of processes;
- Use an automated software tool to test segregation of duties and system access;
- Prospectively test access with the software tool before actually assigning access; and
- Mitigate segregation of duties issues in small facilities.

System Implementations

- Evaluate risks associated with each system implementation; and
- Require self assessments from the process owners.

Management Testing of Controls

- Take a risk-based approach to testing;
- More testing should be done by management;
- Work with external auditors to develop credibility; and
- Reduce the use of external resources.

Evaluation of Results

- Take a risk-based approach to assessment and testing;
- Coordinate testing by management, internal audit, and external audit to identify deficiencies early and reduce their numbers;
- Use the whistleblower process to help identify potential deficiencies;
- Aggregate deficiencies across the organization to identify significant deficiencies;
- Use formal procedures and tools for tracking deficiencies; and
- Follow up on deficiencies identified in prior years.

Section 302 Certifications

- Use management self-assessment to support quarterly Section 302 representations; and
- Use software to streamline the certification process.

Auditor Issues

- Take a top-down approach to auditing to maximize efficiency;
- Work towards a greater reliance on internal audit's testing; and
- Negotiate the timing of external auditor testing to minimize the amount of roll-forward work.

Fostering Future Sustainability

For most companies, compliance with Section 404 of the Act was very costly in 2004, in terms of both time and expense. A March 2005 FEI survey of 217 companies found that employees of FEI member companies logged an average of over 26,000 hours per company during 2004 to comply with the regulations. In addition, member companies spent an average of $4.3 million for added internal staff time and additional fees for external auditors and other consultants. As described in this Executive Report, this time and expense was considered to be necessary to document, test, and audit thousands of individual transactions, so that companies could assert internal control over financial reporting.

During 2005, companies began to look for ways in which to work more efficiently in their compliance efforts. FEI arranged a special discussion session for Section 404 implementation leaders from some of the nation's largest companies, so that they could share their experiences with Section 404. Most participants agreed that the time and expense of compliance during 2004 was not sustainable, and that they would have to look for and implement process improvements.

Some of those process improvements are described in this Executive Report, and include:

- Use a top-down approach to risk and planning;
- Take low risk areas out of scope;
- Use risk assessment to get appropriate coverage;
- Require self-assessment from the process owners;
- Take a risk-based approach to testing;
- Use software to automate documentation, controls, and testing; and
- Work towards a greater reliance on management's testing by the external auditor.

As discussed by the participants, these approaches to Section 404 compliance were process improvements because they helped companies focus on those areas of the business that presented the greatest risk to financial misstatement. The participants agreed that their companies wanted to work more effectively and efficiently as they improved the control environments of their companies.

The May 16, 2005, Policy Statement issued by the Public Company Accounting Oversight Board (PCAOB) was often mentioned during the discussion session held on September 12, 2005. The participants agreed that the recommendations made in this policy statement should encourage closer cooperation between their companies and their external auditors as they looked for ways to more efficiently and effectively document, test, and audit their companies' internal controls.

Introduction

This Executive Report is based on a discussion by 38 Sarbanes-Oxley Section 404 implementation leaders from 33 of the nation's largest companies on their experiences with compliance with Section 404 during fiscal year 2004 and to date in 2005. The discussion session was held in Dallas, Texas, on September 12, 2005, in conjunction with a meeting of the Committee on Corporate Reporting (CCR), a national technical committee of Financial Executives International (FEI). FEI is a leading international organization of 15,000 members, including Chief Financial Officers, Controllers, Treasurers, Tax Executives, and other senior financial executives.

Members of CCR are primarily corporate controllers of Fortune 500 companies, and are responsible for their companies' financial reports.

The format for the one-day discussion session was based on a series of presentations by implementation leaders on the following aspects of Section 404 compliance:

- Key Controls,
- Risk Assessment,
- Segregation of Duties,
- Systems Implementations,
- Management Testing of Controls,
- Evaluation of Results,
- Section 302 Certifications, and
- Auditor Issues.

Implementation leaders made brief presentations on each of these aspects of compliance. Following each presentation, this report's co-author, Dr. Robert A. Howell, Distinguished Visiting Professor of Business Administration from the Tuck School of Business at Dartmouth, moderated a group discussion of other participants' related compliance experiences, and their plans for future compliance.

This Executive Report summarizes the participants' description of their companies' compliance practices during 2004 and to date in 2005, and describes their plans to improve their compliance processes for future sustainability.

Compliance process improvements are described qualitatively in this Executive Report, because the discussion session participants did not try to quantify the benefits to their companies for the other participants.

I. Key Controls

Process improvements for key controls include:

- Identify lower risk areas where reliance on the testing of company level controls is sufficient;
- Critically assess the necessary number of transaction-processing controls;
- Take some lower risk accounts out of scope;
- Reduce the number of testing locations with the use of shared service centers;
- Increase the number of and reliance on automated controls versus manual controls; and
- Find a balance between effective internal control and the number of key controls.

Compliance in 2004

Companies have established a hierarchy of internal controls
A standard hierarchy of controls would include:

- **Entity level controls:** High-level controls that usually support corporate governance, including codes of conduct and whistleblower procedures. Though these types of controls are included in risk assessments, they typically have a minimal effect on scope or transaction level testing. These controls can be used to mitigate other control deficiencies, but are the most difficult to tie to financial reporting.
- **Company level controls:** Mid-level controls for revenue and balance sheet accounts. These controls can be either preventive or detective.
- **Transaction controls:** Low-level controls governing individual transactions.

Most companies relied on too many key controls at the transaction level
Every key control must first be documented, then tested by management, and finally tested by the external auditor. Companies want at least 70% of their revenues and 70% of their balance sheets covered by key controls so that they can assert internal control over financial reporting.

Most companies decided that they had too many key controls at the transaction level in 2004, which then required them to do too much testing at a detailed process level.

Process Improvements for Sustainability

Identify lower risk areas where reliance on the testing of company level controls is sufficient
Routine transactions may be considered low risk and testing every transaction process can be time-consuming and costly. Look for company level controls

(higher than transaction controls) that will mitigate transaction level deficiencies and alleviate the necessity to test routine transactions.

Critically assess the necessary number of transaction-processing controls
Controls on many related transactions may be redundant. By evaluating the transactions and related controls, redundant controls can be combined or eliminated to achieve sufficient coverage.

Take some lower risk accounts out of scope
If an account is considered to have a remote risk of being materially misstated, it can be taken out of scope. The associated controls therefore do not need to be tested on an annual basis.

Reduce the number of testing locations with the use of shared service centers
Shared service centers centralize transaction processing, thereby reducing the number of individual locations where transactions need to be tested.

Increase the number of and reliance on automated controls versus manual controls
Automated controls foster a strong control environment.

Find a balance between effective internal control and the number of key controls
Reducing the number of key controls to be tested will reduce the annual cost of testing, but it may also reduce a company's internal control. Each company will have to find a balance between good internal control and a sufficient number of key controls. Many companies prefer to have some redundant controls, because they have decided that they are necessary for effective internal control.

II. Risk Assessment

Process improvements for risk assessment include:

- Drive audit activity to the highest possible level in the organization;
- Take a top-down approach to risk and planning;
- Use risk assessment to help prioritize businesses and locations to get appropriate coverage;
- Integrate risk assessment with existing ERM initiatives;
- Use shared service centers; and
- Consider the potential for fraud in assessing risk.

Compliance in 2004

Formal company-wide risk assessment is not widespread
Less than 50% of the participating companies did a comprehensive risk assessment during 2004.

External auditors have been risk-averse
The primary guidance for external auditors during 2004 was PCAOB Auditing Standard No. 2 (AS2), "An Audit of Internal Control over Financial Reporting Performed in Conjunction with an Audit of Financial Statements," issued by the PCAOB during the summer of 2004.

Many CCR member companies said that their external auditors applied AS2 in a rigid manner, and did not exercise judgment, so that their audits were detail oriented rather than cost-effective. They said that risk-averse auditors did not encourage a risk-oriented approach to internal control, forcing companies to document and test extensively at the transaction level. In other words, most companies took a "bottoms up" approach to documentation and testing during 2004.

The additional guidance issued by the PCAOB in May 2005 focused on a top down approach in identifying risk areas for internal control testing. However, the audit firms appear to be maintaining a conservative approach, waiting until they have had an opportunity to review the PCAOB's 2004 inspection reports before adjusting their audit approach to reflect this revised guidance.

Process Improvements for Sustainability

Drive audit activity to the highest possible level in the organization
In a top-down approach to internal control, there are fewer key controls at a company level compared to numerous detailed controls at the transaction level. Good internal control can be achieved by testing fewer controls at the company level. However, the company and its auditor should agree on where the risks reside in deciding at what level controls are tested.

Take a top-down approach to risk and planning
The guidance issued by the PCAOB in May 2005 encouraged external auditors to "use a top-down approach that begins with company-level controls, to identify for further testing only those accounts and processes that are, in fact, relevant to internal control over financial reporting, and use the risk assessment required by the standard to eliminate from further consideration those accounts that have only a remote likelihood of containing a material misstatement."

Use risk assessment to help prioritize businesses and locations to get appropriate coverage
In 2004, companies were striving to document and test as many income and balance sheet accounts as possible, because they were being encouraged by their external auditors to do so. Companies are now determining the optimal percentage of accounts that should be covered so that they can assert internal control over financial reporting.

There are a variety of approaches to get to an optimal coverage of revenue and balance sheet accounts. Some companies will focus on key locations in a geographic approach, and some will focus on their most significant financial accounts.

Regardless of the approach, the goal is to focus on those locations or accounts that present the most significant risk to financial misstatement. Some companies will decide to take entire locations out of scope, simply because they do not present a significant risk.

The risk assessment process may therefore reduce the number of physical locations and accounts that need to be included in the company's audit scope. If the risk assessment process thus reduces the number of locations and accounts to be included in scope, it can lead to a limited reduction in required documentation and testing.

CCR company participants generally believe that if their external auditors embrace this risk-based orientation to auditing, executives will be able to take a top-down, or risk-based, approach to internal control.

Integrate risk assessment with existing ERM initiatives
Companies with existing ERM initiatives have already identified potential risks and documented risk mitigation activities. They use these initiatives as a basis for determining what controls are necessary and need to be tested.

Use shared service centers
A shared service center concentrates more activity in one location. Companies can thus achieve greater coverage more efficiently by testing the processes at a shared service center. In addition, processes are controlled more effectively from a single location, which reduces the company's risk of financial misstatement.

Consider the potential for fraud in assessing risk
Fraud needs to be considered in the context of any risk assessment initiative.

Focus attention and testing on those businesses, locations, and transactions with the greatest potential for fraud. Conversely, transactions with less potential for fraud may be taken out of scope.

Leading companies have identified fraud risk factors and are currently reviewing these factors with their divisions. These fraud risk factors will receive special attention during the testing process.

III. Segregation of Duties

Process improvements for segregation of duties include:

- Ensure that all areas that represent key controls have established and sustainable segregation of processes;
- Use an automated software tool to test segregation of duties and system access;
- Prospectively test access with the software tool before actually assigning access; and
- Mitigate segregation of duties issues in small facilities.

Compliance in 2004

External auditors have segregation of duties templates
External auditors have provided some companies with segregation of duties templates for certain processes, such as the revenue cycle or the inventory cycle, so that the companies can check for segregation of duty deficiencies.

Companies have active segregation of duties monitoring programs
Companies track “movers” and “leavers” to monitor who has access to systems. Without an active segregation of duties monitoring program, segregation of duties tends to degrade over time. For example, systems users continue to request access, and more access requests are granted, but people change jobs. Specifically, if an employee had access to the accounts payable system in his old role, but should only be authorized to use the payroll system in his new job, is it a compliance breach to not revoke the accounts payable access once he had moved on to the new position?

Companies have identified segregation of duties security process issues
Companies have identified a number of security process issues related to segregation of duties:

- No defined data or process owners;
- Data/process owners may not understand security;
- Security team may not understand business risks;
- Data/process owners have different views on access;
- Users have different job responsibilities from location to location;
- Segregation of duties may not be a consideration in user and role maintenance; and
- Before the Sarbanes-Oxley Act of 2002, monitoring of segregation of duties was often limited to periodic audits.

Process Improvements for Sustainability

Ensure that all areas that represent key controls have established and sustainable segregation of processes.
Testing, mitigation, and remediation should be focused on key controls. Focus initially on key controls and then work with control owners to test a sample of transactions before finalizing a formal documentation template.

Use an automated software tool to test segregation of duties and system access
With an automated software tool, the user first specifies access rules and inputs a list of individuals, indicating levels of access requested for each individual. The software tool will then print a list of potential segregation violations based upon the rules specified. The user can either choose to remedy a violation by taking the offending access away from an individual, or can choose to mitigate that risk.

The tool does not fix problems, but does provide a detailed segregation analysis and identifies access problems. For best results, users should keep access rules as simple as possible, because segregation of duties can become very complex.

Here are the access rules suggested by one company:

Segregate these functions…	**…from these functions**
Create and change general ledger accounts and cost elements	Make journal entry postings to the general ledger
Setting pay rates Maintaining employee personnel records	Entering time data Cutting checks and/or direct deposit
Enter invoices Pay vendors	Purchasing Receiving
Vendor master maintenance	Enter invoices Pay vendors
Cash application	Sales order/credit memo entry Billing
Sales order/credit memo entry	Billing
Customer Master Maintenance (Accounting View)	Billing Delivery/Distribution Sales Order Entry Payment Processing

Prospectively test access with the software tool before actually assigning access
Software tool users can get a real time analysis of duty segregation by prospectively testing access before access is granted, to see if specific access creates any control issues.

Mitigate segregation of duties issues in small facilities

If a given location has a relatively small number of employees, some of those people may need to have access that would have otherwise been segregated in a larger facility. In these cases, potential segregation deficiencies can be mitigated by a division level review of balance sheet and income statement accounts.

IV. System Implementations

Process improvements for system implementations include:

- Evaluate risks associated with each[MG] system implementation; and
- Require self assessments from the process owners.

Compliance in 2004

Most companies did not permit new system implementations in the fourth quarter
In an informal survey of participating companies, two-thirds did not permit new system implementations in the fourth quarter of 2004.

Process Improvements for Sustainability

Evaluate risks associated with each system implementation
The Sarbanes-Oxley Program Office should evaluate the risks of a new (or modified) system implementation to Sarbanes-Oxley Section 404 assessment or Section 302 certification.

Sample questions to be considered in this evaluation could include:

- Are a number of implementations being planned for a given quarter? (This question addresses the managerial capabilities and capacity of the company's Information Technology [IT] department.)
- Will the system implementation be enterprise wide or just affect a specific location? (This question addresses the materiality of the implementation.)
- Will the system generate key financial information? (Smaller systems that aren't tied directly to the financial statements could be implemented up to fiscal year end.)
- How stable is the system? What are the system's testing results to date? (These question address the risk of bringing the system live.)
- Will the system be tested prior to quarter or year end? (Some companies will not implement a new system in the third month of a quarter, just as they will not implement in the fourth quarter of the year.)
- Are compensating procedures and controls in place? (This question addresses the possibility that the system will fail. Compensating controls are designed to catch errors in a new system.)

Require self assessments from the process owners
Self assessments should be completed by process owners during the development of the system, prior to going live, and immediately following going live. The process owners should do these assessments with assistance from the IT department. Some companies use formal checklists.

V. Management Testing of Controls

Process improvements for management testing of controls include:

- Take a risk-based approach to testing;
- More testing should be done by management;
- Work with external auditors to develop credibility; and
- Reduce the use of external resources.

Compliance in 2004

Most companies use self-assessment
Most companies use a self-assessment tool that is completed by the process owner or other management personnel.

Internal audit does the interim testing at most companies
While internal audit does the interim testing at most companies, the process owner or other management personnel does the testing at other companies. Some companies did continuous testing and others tested two or three times during the year in phases. In general, sample sizes were based on guidance from the external auditors.

There are different approaches to roll-forward testing
If interim testing was done earlier in the year, then roll-forward testing is required later in the year. Some companies used surveys, or simply asked management if anything had changed within their control environment. Other companies did limited testing and followed up on remediated items. Thus, a lot of testing was done in year one.

Process Improvements for Sustainability

Take a risk-based approach to testing
Use risk assessment to prioritize businesses and locations to test on an interim as well as annual basis.

More testing should be done by management
If more testing is done by management, including the process owners and their peer groups, internal audit's time will be freed up for their traditional operational audits and other special audits. Process owners should have the responsibility to do some of their own testing, to make sure that the controls are working as intended. Internal audit can then become more of a quality check.

Work with external auditors to develop credibility
Most companies spent an excessive amount of time and expense on compliance in 2004. For many companies, this time and expense paid off in well-documented internal controls, and the companies developed good credibility with their external auditors.

As external auditors place more reliance on the work of internal audit and the company's control environment, they may be able to reduce the amount of their own testing that will be required.

Reduce the use of external resources
Companies used external resources extensively in 2004 as year one of compliance. These external resources included major auditing firms and other outside consultants.

Once processes are documented and controls are in place and tested, companies will be able to reduce their use of external resources, which are relatively expensive.

VI. Evaluation of Results

Process improvements for evaluation of results and deficiency assessment include:

- Take a risk-based approach to assessment and testing;
- Coordinate testing by management, internal audit, and external audit to identify deficiencies early and reduce their numbers;
- Use the whistleblower process to help identify potential deficiencies;
- Aggregate deficiencies across the organization to identify significant deficiencies;
- Use formal procedures and tools for tracking deficiencies; and
- Follow up on deficiencies identified in prior years.

Compliance in 2004

Companies used multiple sources to identify and evaluate deficiencies
Where work process owners are held responsible for internal control, self-assessment procedures helped identify deficiencies. If the process owner did not identify the deficiency, it was discovered by internal audit testing. Regardless of whether the deficiency was identified through self-assessment or internal audit testing, the work process owner was responsible for analyzing the results and defining an appropriate remediation plan.

Issues were individually prioritized based on magnitude and likelihood
In 2004, companies identified many deficiencies, and had to prioritize those deficiencies to be remediated. They were prioritized based on magnitude and likelihood, and companies focused on those deficiencies that represented the greatest risk to financial misstatement.

Companies were not very sophisticated in tracking deficiencies
Many companies used Excel spreadsheets or Access databases to track deficiencies. They documented the deficiency, the remediation plan, who was responsible for remediation, and the due date. However, this process had limited reporting and analysis capability.

Process Improvements for Sustainability

Take a risk-based approach to assessment and testing
When planning assessments and testing, give priority to those businesses, processes, accounts, and locations that present the greatest risks to the organization, and focus on key controls.

Coordinate testing by management, internal audit, and external audit to identify deficiencies early and reduce their numbers

Management and internal and external audit teams make long lists of processes with the greatest potential risk of deficiency. If these teams can work together to coordinate testing and compare lists earlier in the year, deficiencies can be identified, prioritized, and remediated sooner, rather than at year end. This will help avoid duplication of effort. The goal should be to achieve greater reliance on management testing by the external auditors.

Use the whistleblower process to help identify potential deficiencies

In addition to work process owner self-assessment and internal audit as sources of deficiencies, use the company's whistleblower process as a means to identify control deficiencies.

Aggregate deficiencies across the organization to identify significant deficiencies

Work process owners should be responsible for identifying and remediating deficiencies. However, as deficiencies are prioritized, management needs to monitor similar deficiencies across the organization that may be aggregated into significant deficiencies. Root causes of deficiencies should be addressed, and a formal escalation process should be established to ensure timely remediation.

Use formal procedures and tools for tracking deficiencies

Leading companies use special software solutions to track deficiencies. These integrated solutions have documentation, self-assessment, and remediation tracking and action plan functions, and will categorize deficiencies and link them to specific locations. They also provide enhanced monitoring, analysis, and reporting.

Follow up on deficiencies identified in prior years

Follow up on all outstanding issues identified in prior years. Even if they were minor, they may be symptoms of a weakened control environment, and could potentially be elevated into more significant deficiencies or even material weaknesses in future years

VII. Section 302 Certifications

Process improvements for Section 302 certifications include:

- Use management self-assessment to support quarterly Section 302 representations; and
- Use software to streamline the certification process.

Compliance in 2004

Companies continued their normal Section 302 quarterly certification processes
As mandated by Section 302 of the Act ("Section 302" or "302"), and formalized in a final rule issued by the Securities and Exchange Commission (SEC) in August 2002, companies have been providing CEO and CFO certifications of their annual and quarterly financial statements since 2002. As a basis for these certifications, companies developed in-house certification processes. These processes include sub-entity or divisional certification "roll-ups" and letters of representation.

Some companies have modified their existing 302 certification processes
In 2004, some companies made minor modifications to their 302 certification processes by adding additional language to the 302 certifications related to changes to internal control over financial reporting and increasing the number of management personnel required to complete 302 sub-certifications. Specifically, some leading companies have:

- Developed enhanced processes to identify material changes to internal control over financial reporting through improved questionnaires and checklists, including quarterly control certifications by entity management;
- Integrated 302 quarterly procedures and 404 controls documentation updates, including quarterly reporting of all changes to process documentation;
- Formally defined criteria to evaluate the materiality of changes to internal control over financial reporting; and
- Enhanced integration with information technology to help identify control changes that have occurred as a result of system implementation on a quarterly basis.

At these leading companies, quarterly processes have been formalized to support their 302 certifications and identify material changes to internal control over financial reporting. Groups responsible for identifying material changes to internal control over financial reporting varied, but generally included work process owners, a 404 project management office, management of operating units, and senior management.

Process Improvements for Sustainability

Use management self-assessment to support quarterly Section 302 representations

Some leading companies are not satisfied with their current certification process. They want sub-certifications to be based on self-assessments. In addition, they are conducting quarterly meetings to integrate the results of internal audit testing and management self-assessments to facilitate the analysis of material changes to internal control over financial reporting.

Use software to streamline the certification process

Some leading companies are implementing software to automate the certification process and facilitate the identification of changes to internal control over financial reporting. These companies are also investigating the potential to integrate this process with deficiency tracking software.

VIII. Auditor Issues

Process improvements for auditor issues include:

- Take a top-down approach to auditing to maximize efficiency;
- Work toward a greater reliance on internal audit's testing; and
- Negotiate the timing of external auditor testing to minimize the amount of roll-forward work.

Compliance in 2004

The external auditors tested all controls identified by management
According to most of the discussion session participants, both their companies and their external auditors decided that every process, even at a transaction level, had to be documented, and the related control had to be tested. As a result, in most cases, management identified numerous key controls, and the external auditors tested all of them in 2004.

Neither management nor external auditors used a risk-based approach to testing
When both the companies and their external auditors believed that all transactions, processes, and controls needed to be tested, management and the auditors effectively employed a "bottoms-up" approach to testing, and did not use a risk-based approach. In retrospect, this resulted in inefficiencies in both time and expense.

Reliance on management testing was limited
Because this was the first year in which to comply with new legislation and SEC rules, most external auditors were risk averse and decided to do all testing themselves.

The internal control audit was not integrated with the financial statement audit
Again, because this was the first year in which to comply with new legislation and SEC rules, most external auditors were risk averse. For most companies, the internal control audit was effectively a separate audit from the traditional financial statement audit.

Process Improvements for Sustainability

Take a top-down approach to auditing to maximize efficiency
Most companies agreed that they did not want to continue to pay their external auditors for as many hours worked and billed in 2005 as they did in 2004.

Leading companies are now looking for efficiencies in their external audit. They are now documenting higher level (company) controls, to be tested by both management and the external auditors, which should affect both the timing and extent of testing. A risk assessment of potential financial statement errors should affect the accounts identified as significant and amount of testing required.

Work toward a greater reliance on internal audit's testing
As management develops greater credibility with external auditors, and as the auditors become more comfortable with management's documentation and testing by internal audit, it is expected that the external auditors will place a greater reliance on management's monitoring and internal audit's testing of controls. As a result, the external auditors should be able to limit their work in low-risk areas, and put more focus on non-routine transactions and higher risk control areas.

Negotiate the timing of external auditor testing to minimize the amount of roll-forward work
All companies agree that roll-forward work should be minimized to make the audit as efficient as possible. How this will be done should be negotiated with the external auditor.

For example, some companies say that less risky areas should be audited early in the year, but not so early that they will have to be re-audited later in the year as part of the final audit. Likewise, higher risk areas should be audited early enough to remediate any deficiencies that are identified prior to year end. However, companies have to be careful not to schedule too much testing at year end, during the fourth quarter.

IX. Fostering Future Sustainability

For most companies, compliance with Section 404 of the Act was very costly in 2004, in terms of both time and expense. A March 2005 survey of 217 companies by Financial Executives International (FEI) found that employees of FEI member companies logged an average of over 26,000 hours per company during 2004 to comply with the regulations. In addition, member companies spent an average of $4.3 million for added internal staff time and additional fees for external auditors and other consultants. As described in this Executive Report, this time and expense was considered to be necessary to document, test, and audit thousands of individual transactions, so that companies could certify internal controls over financial reporting.

During 2005, companies began to look for ways in which to work more efficiently in their compliance efforts. FEI arranged a special discussion session for the Sarbanes-Oxley Section 404 implementation leaders from some of the nation's largest companies, so that they could share their experiences with compliance with Section 404. Most participants agreed that the time and expense of compliance during 2004 was not sustainable, and that they would have to look for and implement compliance process improvements.

Some of those process improvements were described in this Executive Report, and include:

- Use a top-down approach to risk and planning;
- Take low risk areas out of scope;
- Use risk assessment to get appropriate coverage;
- Require self-assessment from the process owners;
- Take a risk-based approach to testing;
- Use software to automate documentation, controls, and testing; and
- Work toward a greater reliance on management's testing by the external auditor.

As discussed by the participants, these approaches to Section 404 compliance were process improvements because they helped companies focus on those areas of the business that presented the greatest risk to financial misstatement. The participants agreed that their companies wanted to work more effectively and efficiently as they improved the control environments of their companies.

Many of these concepts can be found in the May 16, 2005, Policy Statement issued by the PCAOB. This policy statement "expresses the Board's view that to properly plan and perform an effective audit under Auditing Standard No. 2, auditors should -

- Integrate their audits of internal control with their audits of the client's financial statements, so that evidence gathered and tests conducted in the context of either audit contribute to completion of both audits;

- Exercise judgment to tailor their audit plans to the risks facing individual audit clients, instead of using standardized “checklists” that may not reflect an allocation of audit work weighted toward high-risk areas (and weighted against unnecessary audit focus in low-risk areas);
- Use a top-down approach that begins with company-level controls, to identify for further testing only those accounts and processes that are, in fact relevant to internal control over financial reporting, and use the risk assessment required by the standard to eliminate from further consideration those accounts that have only a remote likelihood of containing a material misstatement;
- Take advantage of the significant flexibility that the standard allows to use the work of others; and
- Engage in direct and timely communication with audit clients when those clients seek auditors’ views on accounting or internal control issues before those clients make their own decisions on such issues, implement internal control processes under consideration, or finalize financial reports.”

This PCAOB Policy Statement was mentioned often during the discussion session held on September 12, 2005. The discussion session participants agreed that these recommendations should encourage closer cooperation between their companies and their external auditors as they looked for ways to more efficiently and effectively document, test, and audit their companies’ internal controls.

Glossary

Account

An account is a record of debit and credit entries to cover transactions involving a particular item or a particular person or concern, or a statement of transactions during a fiscal period and the resulting balance. In the context of this report, account coverage represents the percentage of balance sheet and income statement account balances that are tested through 404 compliance procedures.

Auditing Standard No. 2

Auditing Standard No. 2, “An Audit of Internal Control Over Financial Reporting Performed in Conjunction with An Audit of Financial Statements,” (AS2) released by the Public Company Accounting Oversight Board (PCAOB) on March 9, 2004. AS2 provides examples of the different orders of magnitude of control deficiencies in its Appendix D. For example, not reconciling inter-company accounts is a control deficiency. Not having a formal process in place to ensure reconciliation would be considered to be a significant deficiency. If there are a significant number of material inter-company transactions, lack of a formal process would constitute a material weakness.

Control deficiency

A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis. (AS2, Paragraph 8.)

Internal controls

Internal controls are the policies and procedures that a company must have in place to ensure that all its assets, liabilities, and transactions are properly reflected on its financial statements.

Material weakness

A material weakness is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the annual or interim financial statements will not be prevented or detected. (AS2, Paragraph 10.)

Process

A process designed by, or under the supervision of, the company's principal executive and principal financial officers, or persons performing similar functions, and performed by the company's board of directors, management, or other personnel, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles and includes those policies and procedures that:

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

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

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

(From AS2, definition of “Internal Control over Financial Reporting,” paragraph 7. See also Securities Exchange Act Rules 13a-15(f) and 15d-15(f).2/)

Scope
The extent of treatment, activity, or influence.

Significant deficiency
A significant deficiency is a control deficiency, or combination of control deficiencies, that adversely affects the company’s ability to initiate, authorize, record, process, or report external financial data reliably in accordance with generally accepted accounting principles such that there is a more than a remote likelihood that a misstatement of the company’s annual or interim financial statements that is more than inconsequential will not be prevented or detected. (AS2, Paragraph 9.)

About the Authors

William M. Sinnett is Director of Research at Financial Executives Research Foundation, Inc. He received a Master of Business Administration from the University of Pittsburgh. Prior to joining FERF, he has held positions in financial management with Mellon Bank and Carnegie-Mellon University.

Dr. Robert A. Howell is Distinguished Visiting Professor of Business Administration at the Tuck School of Business at Dartmouth College. He received his Doctorate of Business Administration in Management Controls from Harvard University. He has combined a career as an academic, consultant, and executive across a broad spectrum of assignments to position himself as a leading authority on corporate governance and financial analysis, reporting, and control practices.

About Financial Executives Research Foundation, Inc.

Financial Executives Research Foundation, Inc. is the research affiliate of Financial Executives International. The purpose of the Foundation is to sponsor research and publish informative material in the field of business management, with particular emphasis on the practice of financial management and its evolving role in the management of business. The mission of the Research Foundation is to identify and develop timely, topical research to advance the financial management profession. The Foundation is an independent 501(c)(3) educational organization. The Foundation receives no portion of FEI Members dues; rather, it relies on voluntary tax-deductible contributions from corporations and individuals.

The views set forth in this publication are those of the author and do not necessarily represent those of the Financial Executives Research Foundation Board as a whole, individual trustees, employees, or the members of the Advisory Committee. Financial Executives Research Foundation shall be held harmless against any claims, demands, suits, damages, injuries, costs or expenses of any kind or nature whatsoever except such liabilities as may result solely from misconduct or improper performance by the Foundation or any of its representatives.

This and more than 80 other Research Foundation publications can be ordered by logging onto http://www.ferf.org

International Standard Book Number 1-933130-19-9

Printed in the United States of America

First Printing

Discussion Session Participants

Diane Allen
Global SOX Lead Manager
3M Company

Cindy Bond
Manager, Internal Controls
McCormick & Company, Incorporated

Tamara Candler
Associate Financial Consultant
Sarbanes-Oxley Coordinator
Eli Lilly and Company

Julie Caponi
Vice President, Audit
Alcoa Inc.

Colleen Cunningham
President and CEO
Financial Executives International

Jeff S. Dawson
Controller – SOX
Georgia-Pacific Corporation

Daniel A. DeRoma
Director, Internal Control Program Office
Eaton Corporation

Kamal Dua
Vice President & General Auditor
Comcast Corporation

Jim Eagen
Director, Professional Development
Financial Executives International

Randi Engelhardt
Director, Business Process Analysis
Cummins Inc.

Saul Gates
SOX Group Manager
Microsoft Corporation

Dr. Joachim Gebhard
Head of Corporate Financial Audit
Siemens AG

Linae Golla
Executive Director of Audit
Tenneco Automotive Inc.

Discussion Session Participants (continued)

Daniel Happer
Executive Director, External Financial Reporting
Time Warner Inc.

David Harris
Audit Manager
The Coca-Cola Company

Ellen M. Heffes
Executive Editor
Financial Executive Magazine
Financial Executives International

Jocelyn Henderson
Assistant Controller
The Washington Post Company

William Hogan
Senior VP, Finance
Computer Associates International, Inc.

Michael Holtman
Director
E.ON AG

Dr. Robert A. Howell
Distinguished Visiting Professor of Business Administration
Tuck School of Business
Dartmouth College

Michael Hultberg
Executive Director, Sarbanes-Oxley
Time Warner Inc.

Gregory A. Jamieson
SOX 404 Manager
The Coca-Cola Company

Nate Jenkins
Senior Financial Advisor
Exxon Mobil Corporation

Beth Karnes
Corporate Manager of Internal Controls
The Coca-Cola Company

Desmond Kealy
Sarbanes-Oxley Controls Manager
Intel Corporation

Anders Land
Chief Internal Control Officer
American International Group, Inc.

Brenda Lovcik
Finance Director
Medtronic, Inc.

Deborah Luening
Northrop Grumman Corporation

Juliana Maglathlin
Director, Financial Projects
Lockheed Martin Corporation

Martha Magurno
Director of Internal Control Compliance
The Dow Chemical Company

Barbara Maloney
Director SOX 404 Project
Motorola, Inc.

Jim Michaelson
Manager, Accounting Policy
Corning Incorporated

John Milliski
SOX 404 Process Leader
E.I. du Pont de Nemours and Company

Dwayne Milum
Director, External Reporting
Wal-Mart Stores, Inc.

Eugene Munson
SOX 404 Project Manager
The Procter & Gamble Company

Kelly Pasterick
Manager, SOX Compliance
Alcoa Inc.

Joseph Reitmeier
Director, Control Assessment
Cummins Inc.

Scott Samels
Manager of Internal Audit
McCormick & Company, Incorporated

Kevin Sierks
Manager, Finance
Guidant Corporation

William M. Sinnett
Director of Research
Financial Executives Research Foundation, Inc.

Discussion Session Participants (continued)

Anupam Tantri
Director, Business Controls
United Technologies Corporation

Steven Vivola
Vice President Finance & COO
J.P. Morgan Chase & Co.

Benjamin White
Director Internal Controls & Compliance
The Black & Decker Corporation

Financial Executives Research Foundation, Inc. would like to acknowledge the following for their support and generosity:

PRESIDENT’S CIRCLE DONORS

Abbott Laboratories, Inc.
ALCOA
AT&T
The Coca-Cola Company
Comcast Corp.
Corning Incorporated
Cummins, Inc.
CVS Corp.
Daimler Chrysler Corporation Fund
Dell Inc.
Dow Chemical Company
Duke Energy Corporation
E. I. du Pont de Nemours & Company
Eli Lilly & Company
Exxon Mobil Corporation
FEI Chicago Chapter
FEI Cincinnati Chapter
FEI Houston Chapter
FEI New York City Chapter
FEI Pittsburgh Chapter
FEI Silicon Valley Chapter
General Electric Company, Inc.
General Motors
Georgia-Pacific Corporation
Hewlett-Packard Company
IBM Corporation
Interpublic Group of Companies, Incorporated
Johnson & Johnson
Lockheed Martin Corporation
Microsoft Corporation
Medtronic, Inc.
Motorola, Inc.
Pfizer, Inc.
Procter & Gamble
Sony Corp. of America
Tenneco Automotive, Inc.
Verizon Foundation

ferf
financial executives
research foundation

business / research

ferf

financial executives
research foundation

Sarbanes-Oxley Section 404 Implementation

Practices of Leading Companies

Sarbanes-Oxley Section 404 Implementation

Practices of Leading Companies

Dr. Robert A. Howell
Distinguished Visiting Professor of Business Administration
Tuck School of Business at Dartmouth

Cheryl de Mesa Graziano
Director of Research
Financial Executives Research Foundation, Inc.

William M. Sinnett
Manager of Research
Financial Executives Research Foundation, Inc.

Sarbanes-Oxley Section 404 Implementation
Practices of Leading Companies

TABLE OF CONTENTS

Sarbanes-Oxley Section 404 Implementation

Practices of Leading Companies

Purpose

Although many aspects of the Sarbanes-Oxley Act of 2002 ("the Act") directly impact financial executives, none caused more effort and costs than Section 404 ("Section 404" or "404").

Section 404 of the Act requires management of public companies to include in their annual reports an assessment of the effectiveness of their financial controls. Compliance with Section 404 includes management's documentation of its internal controls over financial reporting, management's assertion that these controls are effective, and an audit of these internal controls by the external auditor in conjunction with their audit of the financial statements.

While the effort to comply with Section 404 has provided some valuable insights, the time, redeployment of people and other costs associated with the initial implementation is not sustainable. Evaluating the results and understanding leading practices of first year implementation activities in an important step to sustainability.

This report intends to describe the compliance practices of leading companies for a number of aspects of Section 404 as they transition from a "project" orientation to a sustainable "process." It is based on the experiences of the companies that participate on FEI's Committee of Corporate Reporting (CCR).

Executive Summary

Based on their companies' experiences in complying with Section 404 of the Sarbanes-Oxley Act of 2002, participants at a special CCR meeting identified and discussed the following practices:

Organization Structure

- An enterprise wide initiative should be established with a strong tone at the top (e.g., a senior executive "champion").
- Start early, involve many and communicate.
- Finance should take the lead, either from the Controller's department or internal audit.
- Clearly define roles and responsibilities.

- Separate business process documentation from the testing of those processes.
- Provide robust education and training to all involved in the compliance process.

Scope, Documentation, and Testing

- Self-assessment provides a good foundation for process documentation and testing.
- Use a risk-based approach to the determination of scope of documentation, testing and audit.
- Formalize and standardize documentation and testing across business units for both effectiveness and efficiency.
- Internal control reviews should be embedded in the due diligence process.

IT Controls

- The information technology function (IT) should “own” compliance with Section 404 for its systems.
- Develop a common business and IT framework for both business and IT processes.
- Formalize the review process for system additions and changes.

Use of External Resources

- Include the requirement for a SAS 70 Type 2 report in service contracts.
- Negotiate the appropriate timing of the receipt of the SAS 70 report so that it can be included in the audit of internal control over financial reporting.
- Have a contingency plan if a SAS 70 Type 2 report notes some exceptions.

Relationship with the Auditor

- Internal experts should develop their own plan for documentation and testing.
- Encourage open and continuous communication between management, internal audit, and external auditors.
- Involve external auditors in internal audit training sessions.
- Set reasonable milestones.
- Schedule an annual “debrief” between management, internal audit, and external audit.

Deficiency Management

- Proactive identification and prioritization of deficiencies.
- Timely disposition and management.
- Deficiency process owners present remediation plan to management and become responsible for timely remediation.
- Long term sustainability is fostered by training programs.

Audit Committee Communications

- Provide formal reports to the audit committee prior to every meeting on a timely basis.
- Process owners should provide specific examples of control deficiencies to the audit committee, and how they will be remediated.
- The audit committee should hold separate executive sessions with management (e.g., the Chief Financial Officer, the Chief Accounting Officer, and the General Counsel), internal auditors, and external auditors.
- Management should meet with the external auditors to identify lessons learned and present their findings to the audit committee.

Section 302/404 Certification Process

- Operational business units should sub-certify Section 302 reports on a quarterly basis.
- A "Reports by Events" process should be completed quarterly. This is a fact-finding search for any issues that management should be aware of.
- Business units should disclose control issues to corporate management as soon as possible.
- Integrate the Sections 302 and 404 certification processes.

Management Letter and Reporting

- Prepare the management letter on internal control over financial reporting in plain English, so that it can be understood by investors.
- Integrate the management letter on internal control over financial reporting with the existing management letter, if applicable.

Unintended Consequences of Section 404 Implementation

Most companies agree that compliance with Section 404 has resulted in some specific benefits to their individual businesses, such as encouraging a thorough review of existing business processes in their business units. However, most companies also agree that compliance with Section 404 has resulted in some significant unintended consequences:

- Excessive costs of compliance.
- Diversion of management's attention from running the business.
- Changed relationship with external auditors.
- Audit coverage becomes more important than risk.
- Placing restrictions on IT system changes or acquisitions.
- In some cases, U.S. companies have been placed at a competitive disadvantage, particularly when delaying IT system changes that lead to improved customer relationship management.

Introduction

This Executive Report is based on a discussion by 31 Sarbanes-Oxley Section 404 implementation leaders from 27 Fortune 500 companies on their experiences with compliance with Section 404 during fiscal year 2004. The discussion session was held in Boca Raton, Florida, on March 10, 2005, in conjunction with a meeting of the Committee on Corporate Reporting (CCR), a national technical committee of Financial Executives International (FEI).

Members of CCR are primarily corporate controllers of Fortune 500 companies, having the responsibility for their company's financial reports.

The format for the one-day discussion session was based on a series of presentations by implementation leaders on the following aspects of Section 404 compliance:

- Organization Structure,
- Scope, Documentation, and Testing,
- IT Controls,
- Use of External Resources,
- Relationship with the Auditor,
- Deficiency Management,
- Audit Committee Communications,
- Section 302/404 Certification Process, and
- Management Letter and Reporting.

One implementation leader made a presentation on each aspect of compliance. Following each presentation, Dr. Robert A. Howell, Distinguished Visiting Professor of Business Administration from the Tuck School of Business at Dartmouth, moderated a group discussion of other companies' compliance experiences with that topic.

This Executive Report summarizes the practices for each aspect discussed and the individual presentation that was made. During the discussion session, a number of "unintended consequences" of regulations surrounding Sarbanes-Oxley Section 404 were also identified and discussed.

I. Organization Structure

Leading practices for organization structure include:

- Establish a strong tone at the top,
- Start early, involve many executives, and communicate,
- Finance should take the lead,
- Clearly define roles and responsibilities,
- Separate documentation from testing, and
- Provide robust education and training.

Practices of Leading Companies

Enterprise-wide initiative established through a strong tone at the top
Compliance with 404 is not just a finance department responsibility. To be effective, the process must be an enterprise-wide initiative that is championed by senior management and reinforced by the executive tone at the top. Promoting a higher level of understanding of the 404 process at all locations and by non-financial process owners not only stresses the importance of internal controls but further embeds strong controls as part of the corporate culture.

Start early, involve many and communicate
Leading companies started the compliance process early, most in 2003, engaging external auditors, functional areas, and business representation at the onset. Information technology (IT) departments were integrally involved.

Finance takes the lead (Usually the Controller or Internal Audit)
Clearly, finance takes a lead role in managing the process, with many companies introducing a Sarbanes-Oxley controller function at both the corporate and business unit level. Factors such as number of business units, organizational structure, available resources, expertise and flexibility drive a company's decision as to whether the controller's department or internal audit acts as the key finance coordinator of the compliance process.

For example, one company chose to have internal audit lead the process based on their expertise in documenting and testing business processes and because the department had the flexibility of realigning its focus toward 404.

Regardless of the initial approach, most agree that a shift toward process owner responsibility and accountability will occur in 2005 with internal audit achieving a more balanced approach between 404 and operational audits. A third company, for example, asked its business units to enforce compliance and absorb the related costs into their budgets—which the company believes provided impetus to own the process at the business unit level.

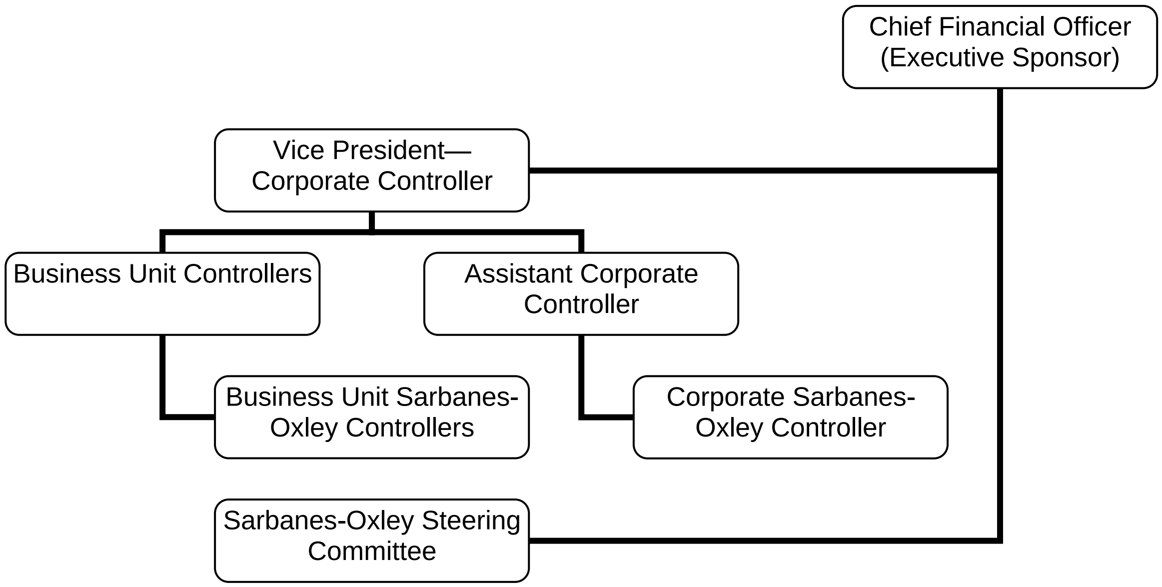
Clearly define roles and responsibilities
Compliance becomes more sustainable the deeper the culture is rooted in internal control. Every job function that affects internal controls needs to clearly understand its unique role and responsibility for the control environment. Leading companies include accountability for internal controls in job descriptions and objectives.

Separate documentation from testing
The importance of process owners taking responsibility for controls is further emphasized when documenting controls. Process owners are responsible for documentation with internal audit testing occurring a layer above each business. Separating documentation from testing provides a more independent check, on which external auditors can better rely. Some companies employ a somewhat modified peer-review approach, using a team from an unrelated business unit or function to review control documentation from another.

Provide robust education and training
Leading companies ensured that all involved were adequately trained, and many companies instituted an internal "SOX certification" process. It is important to sustain this training and update it for additional guidance that might be issued by regulators, as well as for internal changes at the company that may affect the control environment.

Case Study: Company A

The company's Sarbanes-Oxley structure is represented in the following organizational chart.

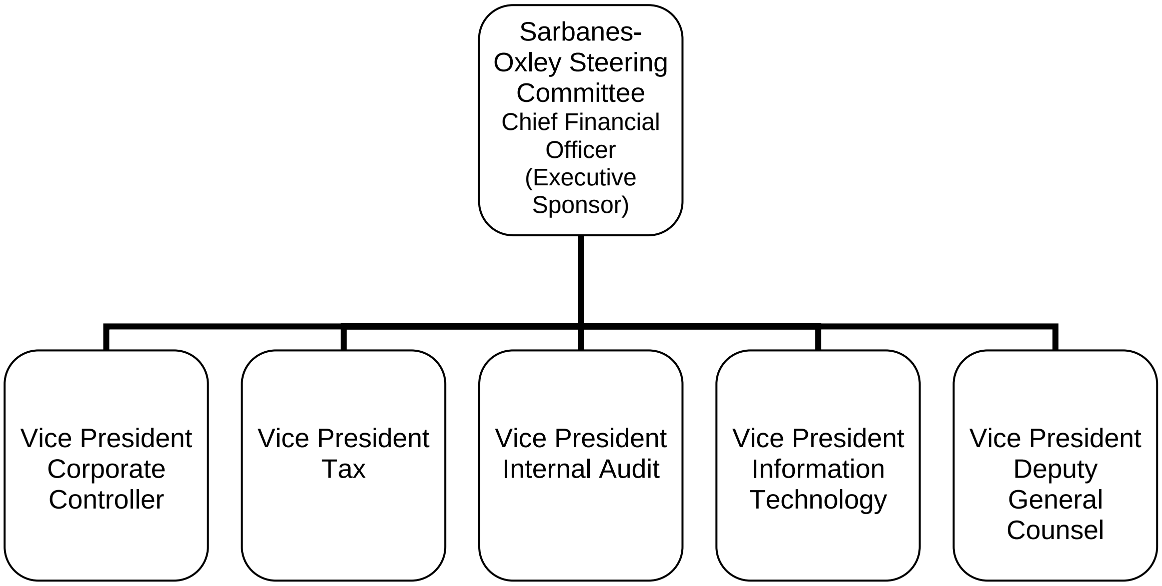


The Sarbanes-Oxley Steering Committee
Company A developed a Sarbanes-Oxley steering committee in early 2003. The chief financial officer was the executive sponsor of the steering committee, and the vice president – controller was the project sponsor. The Section 404 steering committee included five vice presidents:

- Controller,
- Tax,
- Internal Audit,
- Information Technology, and
- The Deputy General Counsel.

The activities of the steering committee were driven by the controller's team. They developed the documentation standards and decided which processes to document.

A visual representation of the steering committee follows:



The Implementation Team

Company A has five business units. Each business unit has a vice president, a controller, a Sarbanes-Oxley controller, and an internal audit director. The Sarbanes-Oxley controller reports to the business unit controller, and the business unit controller reports to the vice president – controller.

Similarly, corporate has a vice president – controller, a Sarbanes-Oxley controller, and a vice president of internal audit. The corporate Sarbanes-Oxley controller reports to the assistant corporate controller.

The vice president – controller's team led the Sarbanes-Oxley Implementation Team, which also included:

- The controller – financial reporting,
- The Sarbanes-Oxley controller,
- The five business unit vice presidents,
- The five business unit controllers,
- The five business unit Sarbanes-Oxley controllers, and
- The five business internal audit directors.

Company A has hired four additional full-time people and shifted the roles of four others to Section 404 compliance. Outside hiring included the Sarbanes-Oxley controller at the corporate and other staff level Sarbanes-Oxley personnel in the businesses and shared services centers.

In implementing the requirements of Section 404, the business unit Sarbanes-Oxley controllers were responsible for business process documentation. The corporate internal audit director and the five business unit internal audit directors removed themselves from this documentation process and focused on the testing of process controls. This allowed the external auditor to rely on the testing performed by internal audit. Significant time was spent in November and December of 2004 following up on testing and remediation testing.

The external audit firm was consulted throughout this process to obtain its agreement with the company's approach to documentation and testing. However, in order to maintain their independence in appearance and in fact, the external audit firm did not provide direct assistance with documentation or templates.

Throughout 2004, the implementation team held weekly meetings with the corporate vice president – controller, the assistant controller, the external auditor, internal audit, and appropriate business personnel responsible for documenting internal controls. They would discuss the status of business process documentation, the testing that had been performed, the testing that needed to be performed, any significant issues discovered during the testing, as well as any necessary remediation work.

The corporate Sarbanes-Oxley controller worked with the business unit Sarbanes-Oxley controllers to improve documentation, testing standards, training, and consistent policies and procedures. He was responsible for consistency in documentation, the testing approach, training, deficiency reporting, remediation, and overall policies and procedures across the five business units.

He was also responsible for consistent communication between the businesses, internal audit, and the external auditor. This approach is critical because Company A has diverse, decentralized business units and more than 50 significant computer systems.

Company A expects to gain efficiencies going forward through the reduction of redundant controls using a combination of risk assessment, cost/benefit analysis, and replacement of manual controls with automated controls. It will seek to automate more controls as it gains a better understanding of its control environment, trains its employees, and implements more common systems.

II. Scope, Documentation, and Testing

Leading practices for scope, documentation, and testing include:

- A self-assessment foundation;
- A risk-based approach to the determination of scope;
- Formalized and standardized documentation and testing; and
- Internal control reviews in the due diligence process

Practices of Leading Companies

Self-assessment foundation

Scoping approaches vary by company. Those that had a pre-Sarbanes self-assessment process that employed a bottom-up approach leveraged the existing structure to comply with 404. This involves owners performing the self-assessment at the business entity or location level. The self-assessment process frequently calls for each location or department to assign itself a risk grade or level that determines if a site and its given controls could be material. The overall 404 team reviews that grade and either agrees with the assessment or asks the locations to make modifications. For business units with lower level risk, a self-assessment questionnaire can be used to document and test controls. Internal audit then performs its own independent assessment.

The companies that did not have an existing formal self-assessment process tended to use a top-down approach in determining what locations and controls fell within the testing scope. From a time-management perspective, companies with a self-assessment foundation had an advantage. However, a top-down approach allows a better focus on the areas of greater risk. A hybrid risk-based approach that focuses on self-assessment combines the advantages of a top-down versus a bottoms-up approach.

Despite the methodology used when determining what controls require more attention, overall importance is placed on the level of risk at each location and obtaining auditor agreement with requirements early on.

Risk-based approach to determination of scope

One issue that surfaced for many companies this first year was the external audit firm's focus on "coverage" ratios for testing (e.g., test 90% of locations) rather than taking a risk-based approach. This caused a disproportionate amount of time spent on documenting and testing controls that wouldn't cause a material misstatement if they were not operating. In response to this, establishing a risk assessment and management process to identify key risks, assess impact, and link to the control environment has become a leading practice.

Formalize and standardize documentation and testing

Leading practice involves establishment of standardized documentation and testing procedures, developed centrally for consistency throughout the company. Use of narrative and flowchart templates and clear instructions accompanying the templates are important in maintaining consistency throughout the compliance process. In addition to clarifying control and testing requirements, self-assessment tools can increase reliance on automated controls where possible and align sampling requirements with external auditor standards. This facilitates not only overall 404 management, but internal audit and external audit reviews as well. Incorporating 404 reviews into the internal audit schedule, so that a single, integrated process further streamlines the process.

Internal control reviews in due diligence process

Internal control reviews are embedded in the due diligence process for new acquisitions. One company considers internal controls in the due diligence process for new acquisitions through performance of internal control gap analysis reviews. This company also developed standard operating procedures to address judgmental areas such as environmental reserves, tax reserves, legal reserves, asset retirement obligations, and goodwill impairment for new acquisitions.

Case Study: Company B

Self-Assessment

Company B has always been very control focused. During the 1990s, it had made a lot of acquisitions and decided that strong controls were not an option, but a requirement.

Therefore, Company B made the decision to develop a self-assessment process for all its businesses throughout the organization back in 1997 and 1998. It had thus already developed in-house, company-specific, self-assessment tools long before Sarbanes-Oxley was signed. These tools included Word documents and checklists, based on the “Internal Control: Integrated Framework” published by the Committee of Sponsoring Organizations (COSO) of The Treadway Commission. This had been a corporate-wide initiative.

These self-assessment tools were updated in early 2004 for Sarbanes-Oxley compliance. Company B went through all of its self-assessment tools, and identified those tools related to financial reporting. These self-assessment modules were then used as a basis for evaluating financial control activities.

Scope of Documentation in 2004

Company B therefore had a “bottoms-up” approach to internal control, with everybody in the organization either performing self-assessment, or at a minimum, being familiar with it.

Self assessment modules were used for financial-process documentation of four different levels of activity in 2004.

Financial and information technology self-assessment modules were used for documentation at all operating locations. Tailored self-assessment modules were used for documentation at service centers and special process centers. Annual testing of this documentation is required, with a September 30 deadline each year. Year end updates to documentation, through December 31, the company’s fiscal year end, can be done with questionnaires, certifications, and resubmission of testing.

Company B created standard operating procedures custom tailored to financial processes at the corporate resource units, which consisted of corporate consolidations, environmental, legal, and tax units. These four organizations had not previously been subject to audit. They had documentation for their processes, but this documentation had not yet been tested. In fact, they did not really understand testing, and a lot of education was required. Going forward, testing here will depend on the frequency of the process.

Finally, standard operating procedures were created for accounting and financial reporting processes, specific to the financial reporting and disclosures. Testing here will be done as close to year end as possible, and prior to the filing of the 10-K.

Risk Assessment

Company B requires annual self-assessments, including updates to documentation and testing controls. An internal audit risk model is used to develop the annual schedule for internal audits. Higher risks require greater audit frequency. For example, derivative financial instrument transactions are audited 6 times per year. If fraud is suspected, the unit is subject to an immediate audit, and there will be a follow up audit within 12 months.

III. IT Controls

Leading practices for information technology (IT) controls include:

- IT owns 404 for its systems;
- A common business and IT framework for both business and IT processes; and
- Formalization of review process for system additions and changes.

Practices of Leading Companies

IT owns 404 for its systems
This report earlier described the importance of involving IT in the compliance process. IT must be integrated into the process, not be separate from it. IT needs to take the lead and own 404 from a system perspective. This includes developing a better understanding of internal control requirements, improving IT control competencies, and continuing to assist with testing and documentation, particularly in the general controls area. This fosters a stronger relationship with finance and supports a risk based approach by resulting in more effective and efficient identification of finance critical systems. For example, one company has assigned one of the key members of the CIO's staff, on a part-time basis, to drive better IT controls, with specific focus on access and change management controls for 2005.

Common business and IT framework for both business and IT processes
Use of a consistent assessment approach is key. During the first year of implementation, most companies used COSO as a basis for their control frameworks from both an overall and an IT perspective. However, based on discussions with external auditors and outside consultants some companies compared their overall approach to other frameworks, such as Control Objectives for Information and Related Technology (COBiT), which focuses on IT controls. Using multiple guidance proved to be a challenge, while concentrating on one assessment approach simplified the compliance process.

Formalization of review process for system additions and changes
Leading practice includes formalization of a process to review significant system additions or changes. This involves communication with and reviews performed by the CIO and internal audit, particularly those systems that significantly affect financial controls. Internal audit reviews can encompass verification of design control and testing before a new system goes live.

Through this preventative action, a company can also drive automated IT application controls. IT general controls can also be automated. For example, one company is looking into company-wide vendor solutions that can assist with managing access controls and application changes. Access-control technology can identify when someone has left the department or the company, automatically remove or transfer system access. Change management solutions assist businesses in tracking and require an approval process for applications changes.

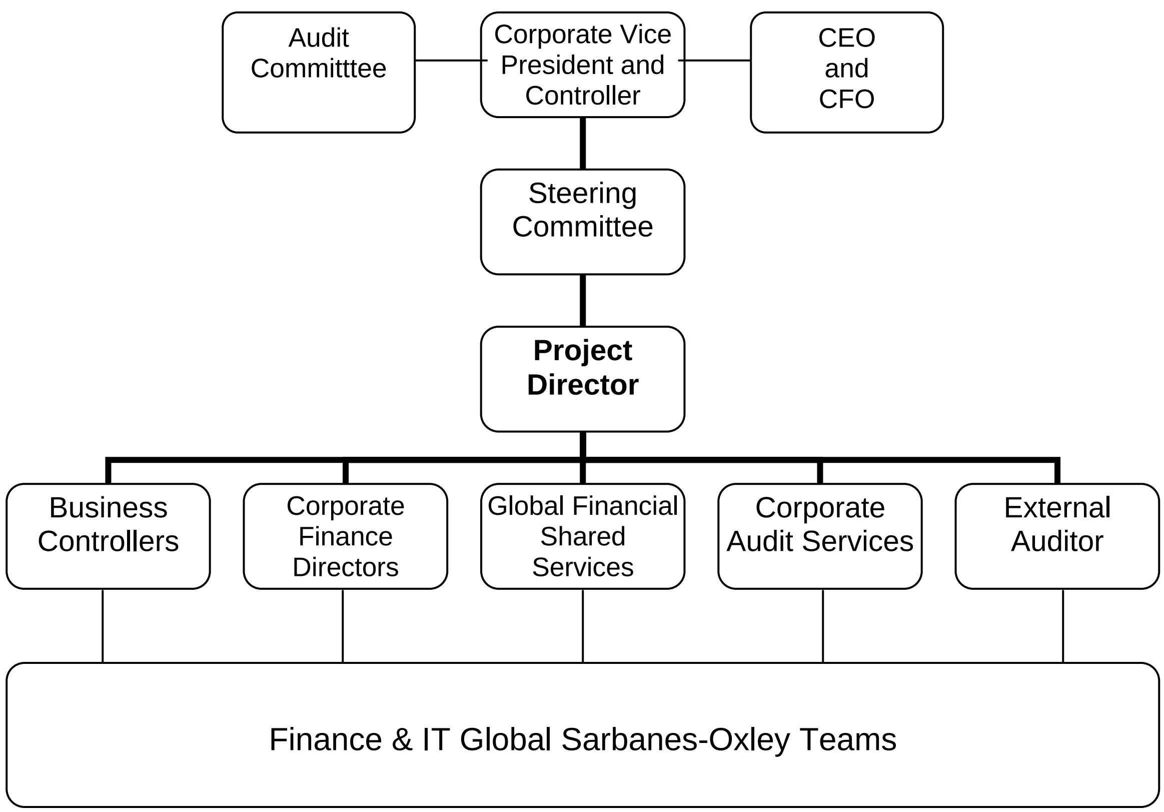
Case Study: Company C

Overview

Company C has four decentralized global business units, each with its own enterprise resource planning (ERP) system. The business operations of all four are very diverse. However, Company C has a centralized, financial shared-service organization. The information technology (IT) infrastructure and operating systems, human resource applications and benefits, and payroll are all outsourced.

The Sarbanes-Oxley project director, who reports to the senior vice president and corporate controller, developed the enterprise-wide assessment standards for Section 404 documentation and compliance. These standards were reviewed by the external auditor and an external consultant, and then put into practice by staff in finance and IT.

A visual representation of the company's Sarbanes-Oxley core team follows:



The IT Approach

The chief information officer (CIO) is responsible for Sarbanes-Oxley compliance for the IT function. He prepares Section 302 and Section 404 sub-certifications for IT and reviews them with the disclosure committee. The disclosure committee includes the senior vice president and controller, the vice president and assistant controller, the vice president of audit services, the vice president of investor relations, and two representatives of the corporate legal department. The disclosure committee then presents these sub-certifications to the CFO and the CEO.

Internal controls to be assessed included:

- Company (entity) level controls,
- IT Database and operating systems,
- Application control, and
- General controls.

Internal audit interviews the CIO and his staff to identify key entity level controls and prepare the necessary documentation. The most important controls concerned IT strategy, IT policies, the qualifications of the IT staff, and relations with outsourcers.

The management of the IT database and operating systems are outsourced, so the Statement on Auditing Standards (SAS) No. 70 Type 2 reports served as control documentation. SAS 70 is an internationally recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA). According to the AICPA, a SAS 70 audit or service auditor's examination "is widely recognized because it represents that a service organization has been through an in-depth audit of their control activities, which generally include controls over information technology and related processes."

Application controls are embedded in the business processes, and therefore are largely automated. These embedded controls were reviewed by assessment teams in the businesses and corporate functions, with some assistance from internal audit.

General controls included access controls, network security, program development and change management. Risk matrices, including risks to management assertions, control objectives, and key control activities, were standardized across the company. Standardized automated test scripts were used to test controls, so that the entire process was highly automated.

Challenges in 2004

The primary IT controls challenge in 2004 was the disruption to the schedule of planned implementations of new IT systems.

Company C realized that, to assure Section 404 compliance by December 31, it would have to delay some IT system implementations planned in the second half of 2004 to the first quarter of 2005. Therefore, it distributed a new IT policy in 2004 mandating that implementations of any new IT systems after August would have to be delayed until 2005. Any exceptions require first the approval of the chief information officer (CIO), and then the disclosure committee, which communicates the exceptions requested to both the CEO and the CFO. This policy is expected to continue into future years.

Several internal systems implementation teams struggled to comply with this new policy by getting new systems up and running by July 2004. It is difficult to complete a system implementation in the fourth quarter, complete the necessary documentation, testing and remediation before December 31.

Results

Company C had effective company level controls, service provider controls (with SAS 70 reports), and network security controls.

The only IT area with significant deficiencies was general controls, specifically access and change management.

Benefits

Company C credits its success with the IT controls to a consistent assessment approach and agreement with the external auditor on the scope and assessment standards early in the compliance process.

Company C also used an external consultant, in addition to the external auditor, and believes that the consultant improved the quality of documentation and testing.

Company C involved all the business units and corporate functions. Not only did this help with the documentation, but it will contribute to the long-term sustainability of effective internal controls.

IV. Use of External Resources

Leading practices for external resources include:

- Inclusion of SAS 70 requirements in service contracts,
- Negotiating the appropriate timing of the SAS 70 report, and
- Developing a contingency plan if a SAS 70 report notes some exceptions.

Practices of Leading Companies

Inclusion of SAS 70 requirement in service contracts
Some vendors do not ask their external auditors to prepare a SAS 70 Type 2 report for their clients. If a company considers the vendor's services to be material to its own system of internal controls, it will need a SAS 70 Type 2 report. The best way to assure receipt of a SAS 70 Type 2 report is to include the requirement in the service contract with the vendor.

Negotiate the appropriate timing of the receipt of the report
SAS 70 Type 2 reports are generally considered to be valid for a period of six months. If the vendor asks its external auditor to prepare a SAS 70 Type 2 report as of December 31, the auditor may not be able to prepare it until, say, February 28, by which time it may be too late to include in internal control testing for the company's internal control audit. However, if the vendor asks its external auditor to prepare a SAS 70 Type 2 report as of August 31 or September 30, the report should be completed in time for the company's annual audit.

Have a contingency plan if a SAS 70 report notes some exceptions
Companies document all the business processes occurring between them and their vendors to show that they are in control of these processes, in case the vendor's SAS 70 Type 2 report notes problems with the vendor's internal controls.

Case Study: Company D

The 2004 Approach

The Company D Sarbanes-Oxley 404 program is run by an Internal Control Program Office (ICPO) consisting of two people. The extended team includes five group Sarbanes-Oxley managers, representing four business units and corporate, respectively. The ICPO has a steering committee, which includes the CIO and an IT member, the vice president and controller, the four main group CFOs, the internal audit director, the ICPO director, the external auditors, and a partner from an accounting firm not responsible for the external audit. Although the company also employed other consultants for IT and its foreign entities, the accounting firm not responsible for the external audit acted as its primary consultant.

Outside Consultants and Software

Toward the end of 2003, the ICPO worked closely with this consultant to develop its internal control framework. Specifically, this included:

- Development and documentation of control objectives,
- Documentation of existing business processes and associated internal control risks and activities,
- Project management of the 404 process, which was subsequently validated by internal audit,
- Use of the consultant's risk control tracking system.

Outside Service Providers – SAS 70

Outside service providers provide the company with material information in three key areas. The following outlines those areas and the attestation approach taken for each:

- Healthcare (medical, dental, disability),
    - SAS 70 Type 2 reports were readily obtained.
- Benefits (401K, pensions, life insurance),
    - SAS 70 Type 2 reports were readily obtained,
    - Testing of existing input and output controls related to data exchange with service providers, along with the work performed if the provider was able to give a SAS 70 Type 2 report.
- IT services,
    - For contracts with entities in the European community that do not issue SAS 70 Type 2 reports, Company D sent external auditors and internal auditors to go through and validate the controls.

Benefits to the 2004 Approach

Company D benefited from the consultants who had more internal control and audit validation knowledge and project management and risk control software experience compared with operations staff.

Challenges Encountered with the 2004 Approach

Working with two big four accounting firms proved to be a challenge given the firms' different views. However, by emphasizing the company's needs, rather than the firms' approaches, the company was able to get everyone on the same page.

Though validation work was completed for entities that could not provide a SAS 70 Type 2 reports, it was a challenge to coordinate the work up front. Timing was also an issue in that some SAS 70 reports in the benefits area were not dated late enough in the year, thus requiring additional control testing as noted earlier.

Changes Planned for 2005

As of the end of February, 2005, the consultants were no longer used. Now, for 2005, the company intends to employ them only on an as needed basis.

The company still stresses importance for internal audit to get involved in validation, so that external audit can rely on its work. However, the audit committee asked that internal audit only spend half of its time on Sarbanes-Oxley audits. The company is also looking for new software to maintain the documentation and controls in 2006.

The company also plans to obtain SAS 70 Type 2 reports on a more timely basis and promote adherence to controls established during the 2004 audit.

V. Relationship with the Auditor

Leading practices for the relationship with the auditor include:

- Internal experts develop plan for documentation and testing;
- Open and continuous communication between management, internal audit, and external auditors;
- Inclusion of external auditors in internal audit training sessions;
- Setting reasonable milestones; and
- An annual debrief.

Practices of Leading Companies

Internal experts develop plan for documentation and testing
Rather than ask for initial guidance for Section 404 compliance from the external auditor, internal experts should develop the company's initial plan for documentation and testing. The external auditor would then need to buy in to this plan. This will assure external auditor independence, which may allow more external auditor reliance on the work of internal audit and management, and encourage the company to be more proactive about compliance. This will also allow the external auditors to provide comments and suggestions on the plan before too much work is done by the company.

Open and continuous communication between management, internal audit, and external auditors
If management, internal audit, and the external auditors meet on a regular basis, the audit process should progress more quickly and efficiently, and issues can be resolved without unnecessary delay. An added benefit is that there should not be any surprises toward the end of the audit.

Inclusion of external auditors in internal audit training sessions
External auditors should be able to rely more on testing done by internal audit if they have an opportunity to see how internal audit is trained in internal control testing procedures.

Setting reasonable milestones
Set reasonable milestones and hold both internal and external auditors more accountable to meeting those deadlines. Monitor progress against milestones and analyze variances, which may be symptoms of audit process problems.

Annual debrief
An annual debrief can be used to identify ways in which the audit can be done more effectively and more efficiently the following year. Management should then provide a report on this debrief to the audit committee.

Case Study: Company E

The 2004 Approach

Company E is a global company with centralized processes.

The Sarbanes-Oxley program office is part of the corporate financial reporting department, which reports to the Chief Accounting Officer. It started documentation in early 2003, but did not hire any outside consultants. Everything was done internally. Internal experts developed a Section 404 compliance plan and presented it to the external auditors. They did not want initial guidance from the auditors, which might impair auditor independence. Instead, the company presented its plan to the auditors and received feedback from them.

Company E developed a partnership relationship with the external auditor, with open and clear communications. The program office, the internal auditors, and the external auditors met on a regular basis to make sure that clear and consistent communications continued through the year and that there were no surprises.

As an example of this partnership relationship, the program office involved the external auditors in the training for internal audit testing.

Benefits to the 2004 Approach

The Sarbanes-Oxley program office dealt with issues early and often, and involved the external auditors upfront, so that there were no surprises. The program office worked with those areas that found control deficiencies, so that those deficiencies could be remediated prior to year end. As a result, there were fewer issues and deficiencies to aggregate at year end. This process also reduced external auditor time.

Challenges Encountered in 2004 Approach

The Sarbanes-Oxley program office set internal deadlines for completing audits, completing testing, and getting feedback, but it was unable to meet those deadlines for a number of reasons:

- Because this was the first year for Section 404 compliance, the program office underestimated the time and effort required to complete the tasks;
- The program office had limited internal staff who could be adequately trained by the time that processes were being tested;
- The program office did not have a streamlined process to review internal audit testing and plan remediation efforts; and
- The external auditors often had to check with their national office before responding to questions.

The Sarbanes-Oxley program office also encountered a significant number of issues with external auditors based outside of the United States, primarily because of lack of training. Another problem was that the external auditors wanted to test the ERP software in every location worldwide, even though Company E had only one ERP system worldwide. The Sarbanes-Oxley program office had to continuously remind the external auditors that the ERP system only had to be tested centrally.

One painful issue in 2004 was the many different IT dependent manual controls and application controls, which had to be first identified and then tested. The external auditors wanted to test every control, whether or not it was a key control. This request generated a major discussion.

There were also many testing inefficiencies. This was the existing process:

- The external auditors would first do their "walkthroughs" at the various locations.
- Internal audit would perform testing.
- The external auditors would perform their testing.
- Finally both internal and external auditors needed to follow up based on initial testing as well as perform roll forward testing.

This redundant process caused much disruption.

Integration of 404 and Annual Audit

To make the audit process more efficient, Company E took several steps to integrate the Section 404 and the traditional annual financial statement audits:

Estimation processes: Walkthroughs, testing, and interim work were performed simultaneously in the fourth quarter to eliminate duplication of effort.

404 testing: Reduced year-end substantive testing based on internal controls testing already performed.

Segregation of duties: Company E pre-populated the external audit checklists to reduce the time required by the external auditor to complete.

Perhaps most important, Company E completed much of its internal control documentation in 2003, which allowed the external auditors to plan an integrated audit for 2004.

As a result of these efforts, there were no surprises during the year-end audit.

Changes Considered for 2005

Based on its experiences in 2004, Company E is considering a number of changes in their compliance process for 2005:

- Push for additional reliance by the external auditors on work and testing done by internal audit teams.
- Set reasonable milestones and hold both internal and external auditors more accountable to meeting those deadlines.
- Establish a more effective communications structure for resolution of deficiency issues and other follow up items.
- Push for more training of and improved communications of expectations with external auditors outside the United States.
- Strive for more effective communication between financial and IT external auditors.
- Develop a more effective testing strategy. For example, combine walkthroughs and testing.

VI. Deficiency Management

Leading practices for deficiency management include:

- Proactive identification and prioritization of deficiencies;
- Timely disposition and management;
- Deficiency process owners present remediation plans to management and become responsible for timely remediation; and
- Long-term sustainability is fostered by training programs

Practices of Leading Companies

Proactive identification and prioritization of deficiencies
In order to proactively identify control deficiencies, the approach should be one of management by prevention. This includes looking at deficiencies at a low level, but analyzing them holistically.

Many companies' management ranked deficiencies based on internal decision-making matrices. These matrices considered factors such as: significance, financial statement impact, magnitude, and likelihood. Such rankings were used to identify the top priorities. This type of ranking process typically includes the involvement of internal and external audit upfront and allows companies to efficiently focus resources toward remediation.

The ranking process generally looks to each process owner to present deficiencies and the suggested remediation to the corporate team, which in turn provided a framework for deficiency aggregation from all sources.

For example, one company employed a deficiency analysis team, made up of its controllers, that looks at the result of managers' testing and performs the pre-aggregation work, which involves looking for themes across the company. The deficiency analysis team presents findings to the company's deficiency classification committee. Comprised of internal audit staff, the CFO, and corporate controller, the committee makes final decisions on remediation efforts. The external auditors also sit on the committee as observers, but do not aid in classifying deficiencies, in order to maintain independence. Though this process has an iterative nature, it leads to alignment and healthy discussion among all parties, and fosters a corporate culture of continuous improvement. It also allows better identification of root causes and the application of sustainable fixes.

Timely disposition and management
Leading companies have a company-wide committee managing an issues file on the deficiency and remediation plan, with frequent updates required from the field. This process served as a basis for reporting any significant deficiencies and material weaknesses upward.

Deficiency process owners present remediation plans to management and become responsible for timely remediation
A leading practice is for the process owner (who could be an operational or finance person, depending on the process) to present the deficiencies deemed to be significant enough to bring to the attention of senior management and the audit committee. This further embeds a culture of accountability for internal controls throughout the organization.

Long-term sustainability is fostered by training programs
A strong training program is essential for prompt identification, management, and disposition of deficiencies. Training can include conducting meetings for all sites that can clarify instructions for the compliance process.

In the long run, a leading practice includes getting cross-functional groups involved, not just finance and IT. For example, existing operating unit controls, such as monthly review of the financials, with manufacturing, procurement, human resources, or plant staff, can get integrated into the control process. This can facilitate timely disposition of control exceptions or issues in the field so that they do not rise to the level of a deficiency. Furthermore, working with cross-functional groups may likely result in streamlining redundant controls through automation and standardization.

Case Study: Company F

The Section 404 Project Office

The Section 404 project office for Company F is headed by the manager of accounting policy. One full time person reports to this manager, and there is also a network of approximately 20 coaches around the world. These coaches include regional financial managers, business controllers, and plant controllers. The effort is supplemented by the work of the internal audit group, which assists in monitoring remediation efforts.

As a matter of policy, the project office "owns" all of the key controls for the company. Changes to key controls must be approved by the manager of accounting policy.

Company F's internal audit function had already been outsourced to a Big Four firm. Another Big Four firm already performs the company's external audit.

2004 Approach – Manage by Prevention

The Section 404 project office started compliance in early 2003, and spent a significant amount of time training people to prepare them for the documentation and testing in 2004.

The project office created centrally a standard set of control documentation which was then distributed to business units. The project management team, including internal audit, discussed the scope of management's assessment plan, documentation and testing that would be required. When this was completed, this information was reviewed with the external auditor. These processes facilitated standardization to minimize variability (and presumably deficiencies) during the audit process.

Timely Disposition and Management

A key goal was to remediate all identified control deficiencies by September 30, 2004. Toward this goal, the project office planned to complete internal audit testing before September 30. If deficiencies were found, they would be remediated and retested early in the fourth quarter. This process reduced deficiencies by over 80% by the year-end assessment.

The project office used a ranking exercise to initially classify deficiencies. While not necessarily an industry practice, this enabled management to quickly elevate potential issues and aggregated findings. They ranked each deficiency identified with a ranking from one to four:

- “One” – very significant, and might be considered to be a material weakness;
- “Two” – potentially a significant deficiency, or a finding which aggregates with other findings to a significant deficiency;
- “Three” – a simple deficiency or test exception; and
- “Four” – not a control deficiency, but rather a negligible error rate (where control objective might still be met).

For each business unit or cycle audit, internal audit prepared an audit report, including information relating to the control issue, and how it would be remediated. These reports facilitated the tracking of deficiencies until remediation was proven.

Benefits to the Approach

The company’s approach benefited the assessment in several ways:

- Significant reduction in total number of findings included in management’s final assessment (80% reduction from initial finding to final population);
- Proactive identification of potential significant deficiencies, which were quickly remediated; and
- Effective use of remediation resources, enabling certain very low-risk deficiencies to flow through to the assessment, with assurance they would not cause a significant deficiency.

Challenges to the Approach

At the time the ranked approach to assessing findings was presented to the external auditors, there was very little guidance in the marketplace as to the general approach to remediation and deficiency management. During the final assessment, there were some challenging auditor discussions relating to the significance of extent of remediation. Recommendation – during the annual planning phase, discuss with external auditors how management will remediate, retest, and conclude upon deficiencies prior to and during the final assessment.

In addition, many of the findings derived from internal and external auditor visits were not accurately characterized in the master list of deficiencies, leading to some confusion in the final assessment of magnitude and likelihood of the deficiencies. Recommendation – ensure deficiencies are accurately stated before the auditors leave the field by conducting closing meetings with site, IT, auditor, and management personnel.

2005 Changes Planned

Company F plans on integrating traditional and information technology significance rankings and deficiency management processes to ensure consistency across the assessment. In addition, management will build out its control gap reporting tool to ensure all attributes of deficiencies are accurately captured.

In line with assessing findings before fieldwork is completed, internal audit staff will determine the potential magnitude and likelihood of findings while the audit progresses, as opposed to waiting until the September 30 remediation deadline approaches. This will enable management to focus efforts where higher risk situations are evident.

In order to manage by prevention, training efforts continue with Company F's coaches network to ensure sites have acceptable control evidence, compensating controls, and effectively monitor performance throughout the year.

VII. Audit Committee Communications

Leading practices for audit committee communications include:

- Providing formal reports prior to every meeting on a timely basis;
- Provide real life examples;
- Executive sessions; and
- Learning from the process.

Practices of Leading Companies

Providing formal reports prior to every meeting on a timely basis
Send the audit committee a formal report at least a week prior to the audit committee meeting. This report should include a project status, control observations with a detailed description of each significant deficiency, and a project timeline. For each significant deficiency, describe exactly what it is, who was responsible for remediation, when it would be remediated, and whether it could become a material weakness.

Provide real life examples
Process owners are responsible for presenting identified control deficiencies and providing updates on the remediation efforts to the audit committee. During each meeting, it is important to provide illustrative examples, engage the committee in dialogue, and obtain agreement on the key risks.

Executive sessions
Ensure the audit committee conducts separate executive sessions with external auditors, internal auditors, and management, including the chief financial officer, chief accounting officer, and general counsel.

Learning from the process
At the end of the compliance process, it is important to engage in a session with the external auditors to identify the lessons learned. These findings should be presented jointly to the audit committee and will result in improvements going forward.

Case Study: Company G

The 2004 Approach

Company G's audit committee meets 10 times each year; six times in person and four by teleconference. One week prior to each audit committee meeting in 2004, Company G's project management office provided a formal Section 404 status report to members of the audit committee. Each report had five main sections:

- Executive Summary,
- Project Status,
- Control Observations,
- Project Timeline, and
- Summary.

Each report was signed by the corporate controller, the vice president of internal audit, and the director of financial compliance.

Company G is decentralized, so the project status section was used to provide members of the audit committee with progress toward completion at each of the business units. The project status section communicated specific status by business unit. A grid was provided in this section that listed for each business unit:

- The number of internal control sub-processes,
- The number of control deficiencies identified by management,
- The number of control deficiencies identified by the external auditors,
- The number of significant deficiencies,
- The percent of deficiencies remediated, and
- The percent of rollforward testing completed.

The control observations section was used to communicate the number of deficiencies identified by either management or the external auditor and the status of remediation activities. After management completed its initial testing in June 2004, the project management office evaluated each control deficiency to determine if it constituted a significant deficiency or a material weakness individually, or in the aggregate. Each significant deficiency was then described in this section (no material weaknesses were identified at Company G). For each significant deficiency, management described the issue and provided a specific corrective action plan, including the individual responsible for remediation and the timeline for corrective action. Each significant deficiency was then included in future status reports until remediation was complete and validated by management and the external auditor. By year-end, all significant deficiencies were remediated and removed from this section of the report.

In November 2004, the project management office delivered a SOX 404 Sustainment Plan to senior management and the audit committee. This formal, 15-page plan on sustainability matters in 2005 and 2006, included the following sections:

- Process Management,
- Control Documentation,
- Control Testing,
- Remediation,
- Reporting,
- Training, and
- Timeline.

Benefits to the 2004 Approach

Company G's project management office notes a number of benefits to this approach. The Section 404 status reports provided timely communication of issues uncovered and progress on remediation throughout the year. Because they were delivered in advance of each audit committee meeting, the actual presentations during the meeting were shorter and resulted in fewer questions.

Additionally, the Section 404 status reports allowed both internal and external auditors to communicate the status of their activities in an integrated package, and the reports kept management accountable for compliance implementation, particularly for the remediation of deficiencies. The reports were well-received by the audit committee members.

Challenges Encountered with the 2004 Approach

The biggest challenge in preparing the Section 404 status reports was getting frequent status reports from the business units. These reports were very important, because the project management office wanted to tell the audit committee what was actually happening in the business units on a near real-time basis.

The next biggest challenge for the project management office was providing "walk in" updates to a status report that had already been mailed in advance. Because there was a lot of testing activity, the controller might have to report more deficiencies at the meeting than were described in the report. These additional deficiencies would then have to be described and explained. These descriptions and explanations would simply add to the information overload.

Deficiency reporting was also a challenge. The project management office used an internally developed framework for evaluating and classifying deficiencies when it first started to report them to the audit committee. This was several months prior to the issuance of the framework that nine auditing firms developed in November 2004. It was also difficult to track and update the status of several hundred deficiencies each month without an automated tool.

Changes Planned for 2005

In 2005, the project management office plans to provide quarterly reports to the audit committee, probably a week before the release of quarterly earnings. Also, the project management office has decided on a consistent deficiency reporting framework with revised templates that are consistent with the auditing firm framework.

VIII. The Sarbanes-Oxley Section 302/404 Certification Process

Leading practices for Sarbanes-Oxley Section 302 and 404 certifications include:

- Operational business units sub-certify on a quarterly basis;
- A quarterly reports-by-events Process;
- Business units disclose control issues to corporate management as soon as possible; and
- Integrate the Sections 302 and 404 certification processes.

Section 302 of the Sarbanes-Oxley Act of 2002 requires the principal executive officer (CEO) and the principal financial officer (CFO) to certify and sign annual and quarterly reports submitted to the Securities and Exchange Commission (SEC). Specifically, the CEO and CFO must certify that:

- The signing officer has reviewed the report;
- Based on the officer's knowledge, the report does not contain any untrue statement of a material fact or omit to state a material fact necessary in order to make the statements made;
- Based on such officer's knowledge, the financial statements, and other financial information included in the report, fairly present, in all material respects, the financial condition and results of operations of the issuer as of, and for, the periods presented in the report.

Further, the signing officers:

- Are responsible for establishing and maintaining internal controls;
- Have designed such internal controls to ensure that material information relating to the issuer is made known to such officers;
- Have evaluated the effectiveness of the issuer's internal controls as of a date within 90 days prior to the report; and
- Have presented in the report their conclusions about the effectiveness of their internal controls based on their evaluations as of that date.

Section 404 of the Act calls for annual reports filed with the SEC to include a statement from the company's management of its responsibility for creating and maintaining adequate internal controls over financial reporting. Management must provide a report including its assessment of the effectiveness of those controls. In addition, the company's external auditor must provide its own opinion on whether it believes the company's internal controls over financial reporting are effective, and must indicate whether it agrees with management's assessment of the company's internal controls.

Practices of Leading Companies

Operational business units sub-certify on a quarterly basis
In order to support the corporate CEO and CFO Section 302 certification of quarterly and annual financial reports, the business unit operational heads and finance heads prepare a similar certification addressed to the corporate CEO and CFO for their business unit, which is their span of control.

Quarterly reports by events process
This is a fact-finding search for any issues that management should be aware of, either from a reporting or disclosure perspective, that aren't automatically identified by the internal control system. These issues should be reported directly to the disclosure committee. The disclosure committee meets before the earnings release to ensure that all appropriate items have been disclosed.

Business units disclose control issues to corporate management as soon as possible
Between the quarterly reporting processes, the business unit heads should disclose any potential issues to corporate management immediately, whether or not those issues represent reportable deficiencies. Corporate can then evaluate all issues disclosed by the business units, evaluate them in total, and decide whether there should be any corporate disclosures.

Integrate the Sections 302 and 404 certification processes
For most companies, compliance with Section 404 was done in addition to their existing processes for compliance with Section 302 in the initial year of implementation.

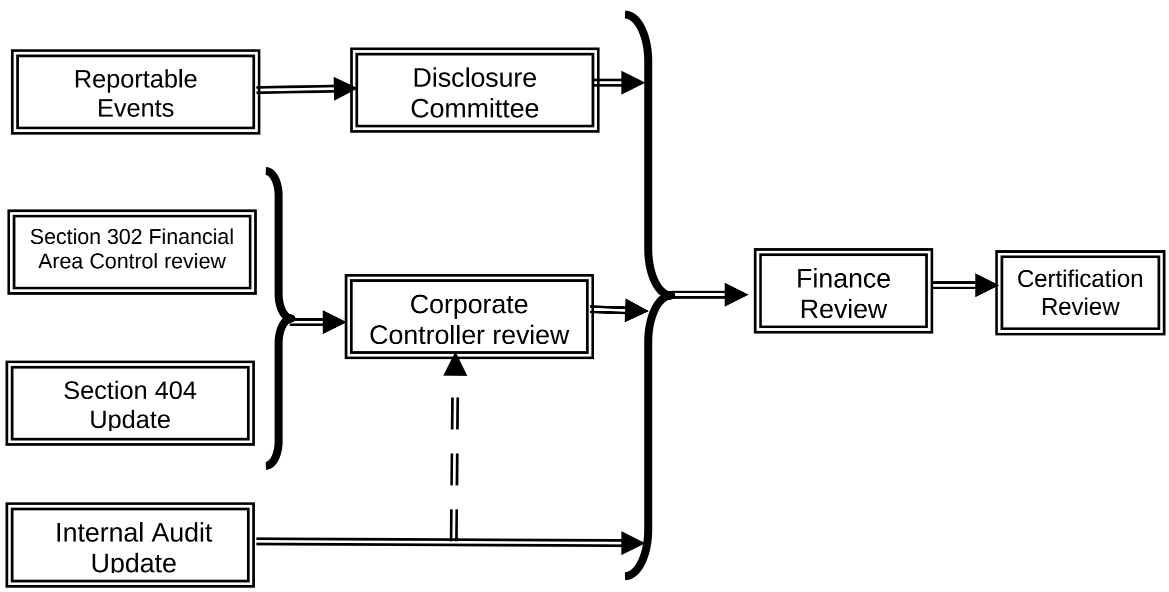
Leading companies include in their certification process a statement that all processes have been documented, that this documentation is current and correct, and that the internal control environment is operating as intended. This certification process makes the business units accountable for their business processes and the related internal controls.

Case Study: Company H

The Section 302 Certification Process

Company H first developed a Section 302 compliance process in 2002, when Sarbanes-Oxley was signed. A Sarbanes-Oxley Program Office was established under the Corporate Controller to lead the Section 302 compliance effort.

The Section 302 compliance process includes four components and is depicted and described as follows:



The first component is the reportable events process. This is a fact-finding search for any issues that need to be considered, either from a reporting or a disclosure perspective. This search is done three times per quarter, and any issues found are forwarded to Company H's disclosure committee. The disclosure committee includes senior managers from finance, legal, and internal audit.

The second component of the Section 302 compliance process is the Section 302 financial review. This is a quarterly review by the business unit controllers of what had changed during the quarter from an internal control perspective, and control deficiencies are identified. Reviews are then held by the business units with the corporate controller.

The third component of the Section 302 compliance process is internal audit, which reviews relevant control deficiencies and allegations of fraud that they identified during the quarter.

Results of disclosure and control work are then consolidated. The corporate controller reviews these results with senior finance, legal, and internal audit management. A certification review is then held with the CEO and CFO.

A 404 update was added in 2004 as a fourth component of the Section 302 compliance process.

The Section 404 Certification Process

The Section 404 compliance process at Company H is headed by a Management Review Committee (MRC), which is comprised of eight members from finance, legal, and internal audit. During 2004, the MRC met once or twice a month.

Reporting to the MRC is the Section 404 Program Management Office, comprised of three members, all managers representing the Sarbanes-Oxley Program Office, Internal Audit, and IT.

The 2004 Section 404 Review Schedule

Meetings

Management Review Committee	Monthly
Audit Committee updates	Quarterly
Certification reviews	Quarterly
Detailed reviews by Executive Management	Annually

Changes for 2005

Company H wants to achieve three fundamental changes in 2005.

Section 404 compliance was “project” based in 2004, but Company H is transitioning from a project approach to a sustaining “process” in 2005. In effect, Company H will change the ownership of the processes to the businesses rather than corporate. The businesses will also be responsible for process improvement and efficiencies.

Company H is driving closer integration with information technology (IT) for better understanding and improved effectiveness between IT and the business units.

Finally, Company H has integrated Section 404 and Section 302 reporting requirements. This required changes in its reporting documentation, but it resulted in just one report from the business units, and this contributed to process efficiencies.

IX. Management Letter and Reporting

Leading practices for the management letter and reporting include:

- Writing the letter in plain English; and
- Interaction with existing report from management.

Practices of Leading Companies

Plain English

Companies prepare the management letter on internal control over financial reporting in plain English, so that it will be more useful to investors and other users of financial statements. Many companies that prepared letters in plain English based their management letters on their previous years' management letters, adding disclosures from a Section 404 perspective.

Interaction with existing report from management

Many companies had an existing report of management included in their annual filings. Most of those that did found that one management letter rather than two letters is more efficient from the standpoint of obtaining senior management signatures and space allocated in the annual report.

Case Study: Company I

The 2004 Approach

Company I provided just one management letter in its 2004 10-K and annual report, covering both the financial statements and internal controls over financial reporting. It originally considered two letters, but thought that the process should be kept simple.

Company I followed an iterative approach to finalize its management letter, starting with the SEC's reporting requirements:

- Management's responsibility for internal controls,
- The framework used by management to evaluate its internal controls,
- Management's assessment of the effectiveness of the company's internal controls over financial reporting, and
- The external auditor's attestation on management's assessment of its internal controls.

However, Company I decided to provide additional disclosures that it deemed important in its management letter, including discussions of:

- Management testing,
- Its control environment,
- Its corporate code of ethics, and
- The activities of its audit and ethics committees.

For the benefit of its investors, the report was written in plain English, stating compliance with SEC regulations, while avoiding legalistic wording. Also, because the external auditor report included a discussion of policies and procedures, these were excluded from the management letter to avoid duplication.

Although the SEC postponed the acceleration of 10-K reporting deadlines by maintaining the 75-day deadline, the company filed within the 60-day window in order to be ready for next year's accelerated reporting deadline.

Challenges Encountered with the 2004 Approach

The company moved the 10-K deadline one week earlier than the previous year, which was a challenge for the overall process. Though the external auditor did not provide a management letter sample, their national office had some last minute edits. Specifically problematic was a paragraph in the letter about evaluation of disclosure controls that was brought forward from the previous year. Had the paragraph been included, the external auditors would have had to qualify the report.

Another challenge was preparing the CEO, CFO, and audit and ethics committees for review and sign-off. At the onset of the annual reporting process, the company responded by:

- Providing a presentation and demonstration of the entire project to the CEO;
- Developing a white paper to answer the audit committee chair’s specific questions; and
- Providing a sample of risks and controls in order to prepare for the review of the 10-K.

Regarding its overall 404 process, the company stressed the importance of having a collaborative 404 team at the top. Its team included an MBA with more management experience, a CPA who acted as the SEC expert, a director of policy operations, and a system expert who ran the compliance program. This allowed the team to be flexible, rather than placing too much reliance on a “superstar.”

X. Unintended Consequences

This first implementation year for compliance with Sarbanes-Oxley Section 404 was marked by a learning curve during which companies, internal auditors, external auditors, and boards of directors redefined their organizational roles and their relationships with one another.

Most companies would agree that compliance with Section 404 has resulted in some specific benefits to their individual businesses, such as encouraging a thorough review of existing business processes. However, most companies would also agree that compliance with Section 404 has resulted in some significant unintended consequences:

Excessive costs of compliance
A March 2005 survey of 217 companies by FEI found that member companies spent an average of $4.3 million for added internal staff time and additional fees for external auditors and other consultants. This average was up 38% from estimates made in July 2004. The March survey results also indicated that employees logged an average of over 26,000 hours per company to comply with the regulations.

Diversion of management's attention from running the business
Generally speaking, focus on Section 404 compliance has resulted in companies' taking more time and effort to get things done, diverting management's attention from running the business. Internal audit resources, in particular, were diverted from activities such as operational audits, systems audits, and special projects, to work on Section 404 activities.

Placing restrictions on IT system changes or acquisitions
In 2004, compliance with 404 has driven some business decisions, such as placing restrictions on IT systems changes or acquisitions during a company's fiscal fourth quarter. Many companies plan to continue such restrictions going forward.

Changed relationship with external auditors
The relationship with external auditors has also changed under 404. In many cases, open, informal interaction has been replaced with more formal and less timely communication, particularly when seeking guidance on technical issues.

Coverage becomes more important than risk-based approach
Another less obvious consequence is the excessive emphasis by company external auditors on obtaining an appropriate "coverage" (e.g., 90% of accounts and locations) rather than taking a risk-based approach to implementation.

In order for Section 404 compliance to move from a “project” orientation to a sustainable process, a risk-based approach to documenting, testing, and monitoring is vital.

Competitive disadvantage

Finally, because of these consequences, US companies believe that they are placed at a competitive disadvantage versus international competitors, particularly when delaying IT system changes that lead to improved customer relationship management.

Glossary

Account
An account is a record of debit and credit entries to cover transactions involving a particular item or a particular person or concern, or a statement of transactions during a fiscal period and the resulting balance. In the context of this report, account coverage represents the percentage of balance sheet and income statement account balances that are tested through 404 compliance procedures.

Auditing Standard 2
Auditing Standard No. 2, "An Audit of Internal Control Over Financial Reporting Performed in Conjunction with An Audit of Financial Statements," (AS2) released by the Public Company Accounting Oversight Board (PCAOB) on March 9, 2004. AS2 provides examples of the different orders of magnitude of control deficiencies in its Appendix D. For example, not reconciling inter-company accounts is a control deficiency. Not having a formal process in place to ensure reconciliation would be considered to be a significant deficiency. If there are a significant number of material inter-company transactions, a lack of a formal process would constitute a material weakness.

Control deficiency
A control deficiency exists when the design of operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis. (AS2, Paragraph 8)

Internal controls
Internal controls are the policies and procedures that a company must have in place to ensure that all its assets, liabilities, and transactions are properly reflected on its financial statements.

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

Process
A process designed by, or under the supervision of, the company's principal executive and principal financial officers, or persons performing similar functions, and effected by the company's board of directors, management, and other personnel, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles (GAAP). It includes those policies and procedures that:

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

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

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

(From AS2, definition of “Internal Control over Financial Reporting,” paragraph 7. See also Securities Exchange Act Rules 13a-15(f) and 15d-15(f).2/)

Scope
The extent of treatment, activity, or influence.

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

About the Authors

Dr. Robert A. Howell is Distinguished Visiting Professor of Business Administration at the Tuck School of Business at Dartmouth College. He received his Doctorate of Business Administration in Management Controls from Harvard University. He has combined a career as an academic, consultant, and executive across a broad spectrum of assignments to position himself as a leading authority on corporate governance and financial analysis, reporting, and control practices.

Cheryl de Mesa Graziano is a certified public accountant and Director of Research at Financial Executives Research Foundation, Inc. She received a Bachelor of Business Administration at Baruch College, City University of New York. She began her career at Coopers & Lybrand and went on to several private-sector positions, including controller and CFO. She has worked for CNBC, Perseus Books, and Bi-Logix, Inc and is completing a master's degree in journalism. Cheryl can be reached at cgraziano@fei.org or (973) 765-1064.

William M. Sinnett is Manager of Research at Financial Executives Research Foundation, Inc. He received a Master of Business Administration from the University of Pittsburgh. Prior to joining FERF, he has held positions in financial management with Mellon Bank and Carnegie-Mellon University. Bill can be reached at bsinnett@fei.org or (973) 765-1004.

About Financial Executives Research Foundation, Inc.

Financial Executives Research Foundation, Inc. is the research affiliate of Financial Executives International. The purpose of the Foundation is to sponsor research and publish informative material in the field of business management, with particular emphasis on the practice of financial management and its evolving role in the management of business. The mission of the Research Foundation is to identify and develop timely, topical research to advance the financial management profession. The Foundation is an independent 501(c)(3) educational organization. The Foundation receives no portion of FEI Members dues; rather, it relies on voluntary tax-deductible contributions from corporations and individuals.

This and more than 80 other Research Foundation publications can be ordered by logging onto http://www.ferf.org

Financial Executives Research Foundation, Inc.
200 Campus Drive
Florham Park, New Jersey 07932

International Standard Book Number 1-933130-04-0
Printed in the United States of America

First Printing

Discussion Session Participants

Leslie Bauer
Director – Internal Audit
The Washington Post Company

Tamara Candler
Sarbanes-Oxley Coordinator
Eli Lilly and Company

Julie Caponi
Assistant Controller – Financial Accounting
Alcoa Inc.

Colleen Cunningham
President and CEO
Financial Executives International

Jeff S. Dawson
Controller – SOX
Georgia-Pacific Corporation

Daniel A. DeRoma
Director, Internal Control Program Office
Eaton Corporation

Kamal Dua
Vice President & General Auditor
Comcast Corporation

Saul Gates
SOX Group Manager
Microsoft Corporation

Dr. Joachim Gebhard
Head of Corporate Financial Audit
Siemens AG

Jay Haberland
Vice President, Business Controls
United Technologies Corporation

James Hall
Manager, Accounting Policy
Exxon Mobil Corporation

Patrick Hamilton
Senior Financial Reporting and Accounting Policy Consultant
Aetna Inc.

Daniel Happer
Executive Director, External Financial Reporting
Time Warner

Discussion Session Participants (continued)

Michael Hardesty
Director, Financial Compliance and Research
Northrop Grumman Corporation

Dr. Robert A. Howell
Distinguished Visiting Professor of Business Administration
Tuck School of Business
Dartmouth College

Michael Hultberg
Executive Director, Sarbanes-Oxley
Time Warner

Gregory A. Jamieson
SOX 404 Manager
The Coca-Cola Company

Desmond Kealy
Sarbanes-Oxley Controls Manager
Intel Corporation

Amy Kwan
Senior Director, Sarbanes-Oxley Group
Cisco Systems, Inc.

Anders Land
Chief Internal Control Officer
American International Group, Inc.

Brenda Lovcik
Finance Director
Medtronic, Inc.

Juliana Maglathlin
Director, Financial Projects
Lockheed Martin Corporation

Martha Magurno
Director of Internal Control Compliance
The Dow Chemical Company

Barbara Maloney
Director SOX 404 Project
Motorola, Inc.

James Michaelson
Manager, Accounting Policy
Corning Incorporated

John Milliski
SOX 404 Process Leader
E.I. du Pont de Nemours and Company

Discussion Session Participants (continued)

Pat Murphy
Sarbanes-Oxley Audit Services Coordinator
Eli Lilly and Company

Kelly Pasterick
Manager, SOX Compliance
Alcoa Inc.

Jeff Perkins
Senior International Audit Manager
The Coca-Cola Company

Joseph Reitmeier
Director, Control Assessment
Cummins Inc.

Scott Samels
Manager of Internal Audit
McCormick & Company, Incorporated

William M. Sinnett
Manager of Research
Financial Executives Research Foundation, Inc.

Mark Slicer
Executive Financial Audit Advisor
General Electric Company

Annette Such
Director of Finance
Guidant Corporation

Benjamin White
Director Internal Controls & Compliance
The Black & Decker Corporation

Financial Executives Research Foundation, Inc. would like to acknowledge the following for their support and generosity:

PRESIDENT'S CIRCLE DONORS

FISCAL YEAR 2005

Abbott Laboratories, Inc.
ALCOA
AT&T
The Coca-Cola Company
Comcast Corp.
Corning Incorporated
Cummins, Inc.
CVS Corporation
DaimlerChrysler Corporation Fund
Dell Inc.
Dow Chemical Company
Duke Energy Corporation
E. I. du Pont de Nemours & Company
Eli Lilly & Company
Exxon Mobil Corporation
FEI Chicago Chapter
FEI Houston Chapter
FEI Pittsburgh Chapter
General Electric Company, Inc.
General Motors
Hewlett-Packard Company
Interpublic Group of Companies, Incorporated
Lockheed Martin Corporation
Microsoft Corporation
Medtronic, Inc
Motorola, Inc.
Pfizer, Inc.
Procter & Gamble
Sony Corp. of America
Tenneco Automotive, Inc.
Time Warner
Verizon Foundation

RESEARCH SPONSORS

FISCAL YEAR 2005

The Board Institute
CSC Consulting
Mellon Consulting, LLC
Paisley Consulting

ferf
financial executives
research foundation

business / research

small public company task force

March 30, 2006

Nancy M. Morris
Federal Advisory Committee Management Officer
U.S. Securities and Exchange Commission
100 F St. N.E.
Washington, D.C. 20549-1090
File No. 265-23

Sent via email to: rule-comments@sec.gov

Dear Ms. Morris,

Financial Executives International's ("FEI's") Smaller Public Company Task Force ("SPCTF") is pleased to respond to the Securities and Exchange Commission's (SEC's) Request for Comment on the Exposure Draft (ED) of the SEC Advisory Committee on Smaller Public Companies (the "SEC ACSPC") released on February 28, 2006 (Release No. 33-8666).

FEI is a leading international organization of 15,000 members, including Chief Financial Officers, Controllers, Treasurers, Tax Executives and other senior financial executives. SPCTF is an FEI task force that was created to address the recommendations of the SEC ACSPC. The task force represents the views of smaller public companies. This document reflects the views of FEI's SPCTF, and not necessarily the views of FEI or its individual members.

SPCTF recognizes the significant level of time and effort the SEC ACSPC expended over the past year. The in-depth research gathered at the numerous public hearings is reflected in the recommendations and background provided in the ED. We commend the SEC for supporting this effort. SPCTF comments on specific recommendations are detailed below.

I. REPORTING ON INTERNAL CONTROL OVER FINANCIAL REPORTING

SPCTF recognizes the SEC ACSPC recommended full exemption for microcaps and partial exemption for small cap companies (pertaining to the auditors's report) from Section 404 and the majority of its members support such exemptions. SPCTF believes that the concerns raised to date with respect to the cost-benefit equation of Section 404, particularly as implemented under existing SEC and PCAOB rules, are particularly exacerbated for smaller companies.

We note that Recommendation III. P. 1 of the ED also recommends that "management should be required to report on any known material weaknesses" and the ED states that "the Proposed Statement on Auditing Standards of the AICPA, "Communications of Internal Control Related Matters Noted in an Audit," if adopted by the AICPA and the PCAOB, would strengthen this disclosure requirement and provide some external auditor involvement in the internal control over financial reporting process."

We believe further study is necessary to determine if the above proposed standards of the AICPA would be appropriate or necessary in light of existing SEC standards for disclosure by public companies. We believe further study is needed from the preparers' and investors' point of view.

FEI's SPCTF agree with the recommendation in the ED that further guidance is needed to address the core issue identified by the SEC ACSPC: to improve the cost-benefit equation of complying with Section 404.

Such guidance should come in the form of "right-sizing" AS2 in a separate standard directed at smaller companies in particular, or through "right-sizing" AS2 to address the needs of small and large companies. The "right-sized" standard can reflect learnings of the SEC ACSPC as well as information provided at the upcoming May 10, 2006 SEC-PCAOB roundtable.

In addition, consideration should be given as to whether the SEC needs to issue further guidance for management, and smaller public company management in particular. As has been widely noted, the SEC's management reporting rule under Section 404 provided sparse guidance for management, and the auditing standard (AS2) became the de facto guidance. Although the Committee Of Sponsoring Organizations (COSO) is developing guidance for smaller public companies, it is not yet final and it is unclear whether such guidance will be helpful to smaller public companies in its final form.

II. MICRO CAPS AND SMALL CAPS SHOULD HAVE THE OPTION TO PROVIDE A DISCLAIMER

As an alternative to the ED's recommendation for exemptions of smaller public companies, and in addition to our concurring that further guidance is needed, SPCTF believes that smaller public companies should be allowed an option of providing a "disclaimer" (similar to that for the listing requirements for boards of public companies) to state if they are unable to provide a Section 404 management or auditor's report.

Such a disclaimer would have to provide the reasons why the Section 404 report(s) could not be filed, and would have to be certified by the company's Principal Executive Officer (generally, the Chief Executive Officer or CEO) and the company's Principal Financial Officer (generally, the Chief Financial Officer or CFO), in conformity with the signature requirements for the Section 404 reports and Section 302 certifications.

Further consideration would have to be given to SEC filing status and stock exchange listing requirements, for companies that file their 10-Ks without a Section 404 report, and with a disclaimer only.

III. MORE GUIDANCE SHOULD BE ISSUED BY THE SEC WITH RESPECT TO MATERIALITY

SPCTF supports the ED's recommendations that the SEC issue further guidance with respect to materiality, especially the use of quarterly (versus annual) materiality for purposes of accounting recognition and disclosures relating to prior period restatements.

IV. DETERMINE THE NECESSARY STRUCTURE FOR COSO

The ED states this is necessary because COSO has been placed in an "elevated role" by virtue of its reference in the SEC rule on management reporting and in PCAOB's AS2. The ED further recommends that the SEC, "in conjunction with other interested bodies, as appropriate, should determine the necessary structure for COSO, including a broader member constituency, to strengthen it in light of its important role in establishing and providing guidance with respect to the internal control framework used by most companies and auditors to evaluate the effectiveness of internal control over financial reporting."

We do not believe it is appropriate at this time for COSO to become a standard setter. COSO is undergoing its own strategic planning process, and we support that effort.

We do not agree that the status of COSO has been “elevated”. COSO has been the predominant internal control guidance used in the U.S. since 1992. However, COSO is not a standard-setter in the sense of the regulators and standard-setters such as the SEC, PCAOB, and FASB. The strength of COSO has been, by its very nature, as a private sector initiative. If COSO were to be elevated as a standard-setter, it will potentially preclude the direct participation of private sector sponsoring organizations, which includes FEI. One of the complicating factors with respect to Section 404, has been, as widely noted, the lack of specific guidance for management in the SEC rule, the default to PCAOB’s AS2, and the resultant request that COSO issue guidance for management, specifically small company management.

Based on reading COSO’s ED issued in October 2005, comment letters filed in response to the ED, and the other findings in the SEC ACSPC’s report, much of the current approach to Section 404 is, as it should be, derived from and limited by the requirements of the SEC’s and PCAOB rules (standards); thus, the COSO 1992 Framework may not have been at issue, as much as the SEC’s and PCAOB’s rules themselves, which are most properly considered directly by the SEC and PCAOB, not by the COSO guidance.

V. PRINCIPLES-BASED (OBJECTIVES-BASED) ACCOUNTING AND REDUCING COMPLEXITY

The SEC should formally encourage the FASB to continue pursuing objectives-based accounting standards. Microcap companies should be permitted the same delayed effective date as private companies.

SPCTF supports the ED’s recommendation that the SEC once again formally encourage the FASB to continue to pursue objectives-oriented accounting standards. We also commend the SEC ACSPC for addressing the importance of combating complexity by further specifying in its recommendation, in addition, simplicity and the ease of application should be important considerations when new accounting standards are established**.** FEI’s SPCTF supports the recommendation that microcap companies should be permitted the same delayed effective date as private companies.

Thank you for considering our views. We would be happy to discuss this further at your convenience or respond to any questions you may have. Please feel free to contact Serena Dávila at sdavila@fei.org, (202) 626-7809 or Rick Brounstein at broun@comcast.net, (510) 774-1969 should you have any questions.

Sincerely,

Richard D. Brounstein

Richard D. Brounstein
Chairman, Smaller Public Company Task Force (SPCTF)
Financial Executives International
Member, SEC Advisory Committee on Smaller Public Companies