

**A LAYPERSON'S GUIDE**  
**TO**  
**INTERNAL CONTROL OVER FINANCIAL REPORTING**  
**(ICFR)**

Prepared by Kayla J. Gillan,  
Member of the  
Public Company Accounting Oversight Board  
For  
The Council of Institutional Investors'  
Annual Spring Meeting

March 31, 2006

*The views expressed in this document are those of the author's, and do not necessarily reflect the position of the PCAOB, its other Board members, or its staff.*

## TABLE OF CONTENTS

	<u>Page</u>
WHAT IS “INTERNAL CONTROL OVER FINANCIAL REPORTING” (ICFR)?	1
WHAT IS A “MATERIAL WEAKNESS” IN ICFR?	2
WHAT DOES IT MEAN FOR A COMPANY TO HAVE A “CLEAN” AUDIT OF ITS FINANCIAL STATEMENTS, BUT DISCLOSE ONE OR MORE MATERIAL WEAKNESSES IN ICFR?	3
WHAT IS COMPANY MANAGEMENT’S RESPONSIBILITY WITH REGARD TO ICFR?	4
WHAT IS THE INDEPENDENT AUDITOR’S RESPONSIBILITY WITH REGARD TO ICFR?	5
HOW DOES THE TESTING PERFORMED DURING THE §404 PROCESS RELATE TO THE FINANCIAL STATEMENTS’ AUDIT?	6
CURRENT ISSUES	7
COST & BENEFIT CONSIDERATIONS	9
OPPORTUNITIES FOR INPUT	12
WHERE TO GO FOR MORE INFORMATION	13
<u>APPENDIX</u>	
1. REPRINT OF §404 OF THE ACT	16
2. EXCERPT OF §103 OF THE ACT	17



## WHAT IS “INTERNAL CONTROL OVER FINANCIAL REPORTING” (ICFR)?

“Internal controls” refer to those procedures within a company that are designed to reasonably ensure compliance with the company’s policies. Under the framework developed in the early 1990s by the Committee on Sponsoring Organizations (COSO)<sup>1</sup>, there are three types of internal controls:

- Those that affect a company’s operations
- Those that affect a company’s compliance with laws and regulations
- **Those that affect a company’s financial reporting**

Frequently, a control may address more than one of these objectives. This paper focuses **only** on those controls that affect a company’s financial reporting; this is also the sole focus of §404 of the Sarbanes-Oxley Act of 2002 (the Act).

Under the COSO framework, there are five interrelated “components” of an effective internal control system; these are derived from the way the company is managed on a day-to-day basis:

1. The company’s top-level environment with respect to control. This includes elements such as the ethical “tone at the top,” and the effectiveness of the board’s audit committee in its high-level oversight of financial reporting. This component is known as the Control Environment.
2. The assessment of risks of the various processes and data points that feed into the company’s financial reports. For example, a process that is highly susceptible to fraud would be considered to be a high-risk area.
3. The way in which controls are actually designed and implemented within the company, so as to address the identified risks. This component is known as Control Activities.
4. The way in which information within the company is gathered and shared, both to people within the company responsible for financial reporting, and to external users of financial reports. This component is known as Information and Communication.
5. The way in which the effectiveness of these controls are monitored by company management.

---

<sup>1</sup> COSO was formed in 1985 to sponsor the National Commission on Fraudulent Financial Reporting (the Treadway Commission), and consists of organizations of financial executives and auditors.

## WHAT IS A “MATERIAL WEAKNESS” IN ICFR?

A material weakness in ICFR exists if there is some flaw within the company’s overall control system such that it is **at least reasonably possible** that a **material misstatement** in the company’s financial statements will not be prevented or corrected. Such a misstatement may occur on an annual basis (either before or after an audit [*see question below*]), or through interim financial reporting (e.g., quarterly reports, which are un-audited). Examples may include inadequate segregation of duties (e.g., the person that receives commission from a sale also approves the loan agreement and reconciles the bank account); personnel lacking in sufficient accounting expertise to accurately prepare the financial statements; and failure to reconcile significant account balances.

Under existing SEC and PCAOB rules, material weaknesses in ICFR must be publicly reported. Flaws in control systems that fall below “material” are reported within the company, either to company management or the audit committee (depending upon the severity of the flaw). In evaluating the severity of a flaw in ICFR, both auditors and companies look at two factors: the **likelihood** that the flaw will result in a financial misstatement, and the **magnitude** of such an outcome. Thus, this process is, in essence, an exercise of risk analysis.

For ICFR purposes, the meanings of “reasonably possible” and “material” rely upon long-established definitions of these same terms that exist with respect to accounting. However, experience gathered during the first year of implementing §404 and AS2 demonstrate that auditors and companies both had a difficult time applying these terms in this new context. Like the generally accepted accounting principles (GAAP) that govern the preparation of financial statements, there are no clear bright-line tests based solely on quantitative measures; qualitative measures must also be considered, and professional judgment is required.

**WHAT DOES IT MEAN FOR A COMPANY TO HAVE A “CLEAN” AUDIT OF ITS FINANCIAL STATEMENTS, BUT DISCLOSE ONE OR MORE MATERIAL WEAKNESSES IN ICFR?**

When an independent auditor issues a “clean” opinion on the company’s financial statements, this is a representation to the public that the auditor has followed applicable auditing and related professional standards so as to allow the auditor to conclude with reasonable assurance that the financial statements are fairly presented in conformity with GAAP in all material respects. A “clean” audit opinion is not a guarantee of error-free financials, but is rather the conclusion by an auditor – using procedures and professional judgment that are reasonable to the circumstances – that the statements are fairly presented.

But, neither the auditor nor the company is required to disclose whether the **audit process itself** revealed financial statement errors that were corrected before the statements were filed with the SEC. The degree to which the auditor is involved in requiring management to correct financial statements prior to their public filing is an indication of whether the company – *using only its own personnel (either employees or third party consultants)* – will produce financial information that is materially accurate. The ability of a company to accurately describe its own financial condition is particularly relevant when the company discloses un-audited financial information, as in quarterly reports filed with the SEC. Thus, while the audit of a company’s financial statements may be “clean,” this provides little information to those outside the company as to whether other financial information is of similar reliability.

One of the key purposes of §404 is to provide this additional information to market participants. Specifically, the ICFR audit report provides the public with a barometer against which to evaluate the reliability of a company’s disclosed financial information. Auditors follow certain professional standards (principally contained in PCAOB Auditing Standard No. 2 [AS2]) both to be able to reach a conclusion about the effectiveness of a company’s ICFR, and to report that conclusion to the public.

## WHAT IS A COMPANY'S RESPONSIBILITY WITH REGARD TO ICFR?

Since the enactment of the Foreign Corrupt Practices Act of 1977 (FCPA), every US-traded company (regardless of size and place of operations) has been required to create a system of "internal accounting controls". In its rules implementing the FCPA, the SEC has explained that this responsibility requires that companies:

- Maintain books, records, and accounts which, in reasonable detail, accurately and fairly reflect the company's transactions; and
- Devise and maintain internal controls sufficient to provide reasonable assurance that:
  - Transactions are executed in accordance with management authorization;
  - Transactions are recorded as necessary to (a) permit preparation of financial statements in conformity with GAAP and (b) maintain accountability for assets;
  - Access to assets is permitted only in accordance with management authorization; and
  - Recorded accountability for assets is compared with the existing assets at reasonable intervals, and appropriate action is taken regarding any differences.

The Sarbanes-Oxley Act of 2002 enhanced this responsibility in two ways. First, §404(a) of the Act [*see Appendix A-1*] requires a large subset of these same companies to annually report on the company's own assessment of the effectiveness of these controls. Second, under §302 of the Act, certain corporate officers must (among other things) accept responsibility (as evidenced by individual signatures) for the content of the company's annual §404(a) report.

US-domiciled companies with public float over \$75 million (also known as "accelerated filers") have been required to comply with the new reporting rules for annual reports covering fiscal years ending after November 15, 2004. The comparable compliance dates for non-US accelerated filers is July 15, 2006, and for all smaller companies is July 15, 2007.

## WHAT IS THE INDEPENDENT AUDITOR'S RESPONSIBILITY WITH REGARD TO ICFR?

Auditors, too, have been familiar with the concept of internal controls for years. For decades, auditors have been required to understand the company's ICFR; this understanding, in turn, was to be used by the auditor to tailor the "nature, timing and extent" of the auditor's testing with regard to the company's *financial statements' audit*. For example, if an auditor found a company's ICFR to be poor, the auditor should have responded by performing more extensive testing, or pursuing tests that result in more persuasive evidence (e.g., written vs. oral evidence). However, the auditor's awareness of significant flaws in a company's internal control systems provided no incentive for the company to correct the flaws; the auditor was simply expected to "audit around" the flaws.

Under §404(b) of the Act [*see Appendix A-1*], independent auditors are now required to "attest to, and report on" the company's §404(a) assessment. This requirement of public disclosure, by both the company and the auditor, now creates a strong incentive for company self-correction.

As in any attestation, for an auditor to attest to managements §404(a) assessment, the auditor must gather evidence to test whether management's assertion that its ICFR is effective is correct. The auditor's scope of review is not limited to looking at the process that the company used for its assessment, however. This point – challenged by some – is confirmed by §103 of the Act [*see Appendix A-2*]. Section 103 directs the PCAOB, in fulfilling its standards-setting responsibility, to adopt a standard requiring that the auditor report on (among other things) "the scope of the auditor's testing of the internal control structure and procedures of the issuer, required by §404(b)." Moreover, under §103 this report must also include the auditor's findings; an evaluation of the company's internal control structure and procedures; and a description of any material weakness in ICFR. All of these items are specifically to be based on the auditor's testing.

AS2 is the PCAOB auditing standard designed to fulfill both §103's and §404(b)'s requirements.

## **HOW DOES THE WORK PERFORMED DURING THE ICFR AUDIT RELATE TO THE FINANCIAL STATEMENTS' AUDIT?**

The audit of a company's financial statements and the audit of that company's ICFR must be performed by the same auditor, and the two audits should be integrated. With integrated audits, the tests that the auditor performs may serve two purposes.

Illustration A: In an audit of ICFR, the auditor is required to "walk-through" at least one transaction within each significant class of transactions. A "walk-through" represents a "soups-to-nuts" review of how a transaction begins (e.g., with a customer order) to how it is recorded on the company's books and, finally, to how the transaction ultimately flows through to the financial statements. When performing such a walk-through, the auditor gains first-hand knowledge of the points in this process at which material misstatements could occur. This understanding also allows the auditor to design a more effective strategy for auditing the financial statements than if no walk-throughs had been performed.

Illustration B: During an ICFR audit, the auditor will assess the risks of a material weakness arising in various places within the company's overall financial reporting system. When designing and implementing procedures to test the effectiveness of controls in these areas, the auditor may find that these same procedures are also helpful to the financial statements' audit; in such a case, the procedures need only be performed once.

Both of these examples illustrate how this integration not only results in a higher quality financial statement audit, but also provides the opportunity for the auditor to be efficient with his/her time.

## CURRENT ISSUES

During AS2's first year of implementation, participants in the ICFR process raised a number of issues that put in question both the manner in which auditors performed their work, and whether this work provided value in excess of its cost. Were auditors too granular in their review of ICFR? Were auditors pushing company management to take a minute, rather than material approach? Were the costs of the Act's internal control requirements outweighing the benefits?

As a result of these and other questions, on May 16, 2005 the SEC and PCAOB each issued clarification to both companies and their independent auditors. Among other issues, this guidance addressed the need to analyze ICFR using a "top-down" and "risk-based" approach. In addition, the PCAOB pledged to use its inspection program to review how, in fact, auditors were fulfilling their ICFR responsibilities. A PCAOB report on these findings was issued on November 30, 2005. (See [www.pcaobus.org](http://www.pcaobus.org).)

Now, as the second year of AS2 implementation for most US large companies nears an end, it is appropriate to step back and again ask questions: Are auditors doing the work required of them? Perhaps even more fundamentally, are the auditor requirements achieving the desired end-result of greater transparency around the state of company controls? At what cost? These questions, and others, will be explored at a SEC/PCAOB roundtable to be held on May 10, 2006.

As a related matter, in December 2004 the SEC established an Advisory Committee on Smaller Public Companies and charged it with examining, from a cost-benefit perspective, the impact of federal securities laws on smaller companies. This Committee's draft recommendations are open for public comment until April 3, 2006, after which the Committee will submit its final recommendations to the SEC. As to ICFR, the Committee's draft recommendations are to exempt (at least temporarily) certain companies from one or more parts of §404. The table on the next page summarizes these recommendations:

**Summary of Advisory Committee on  
Smaller Public Companies Draft Recommendations**

Market Capitalization	Annual, or Annual <i>Product</i> Revenue	Recommended Exemption
Less than \$128 million (called “micro cap”)	<\$125 million annual revenue	All of §404, on the condition the companies adopt governance standards that generally parallel those applicable to listed companies, and that companies report on any known material weaknesses in ICFR
Less than \$787 million (called “small cap”)	<\$10 million in annual <i>product</i> revenue	
“Small cap”	<\$250 million annual revenue, but >\$10 million annual <i>product</i> revenue	§404(b)/auditor requirements (with the same condition stated above)
“Micro cap”	Between \$125 and \$250 million annual revenue	
<p>If the SEC declines to provide the exemptions as described above, then the alternative draft Committee recommendations call for the SEC to direct the PCAOB to adopt a different ICFR auditing standard for smaller companies, requiring that auditors only look at the design and implementation of ICFR (rather than also testing operating effectiveness). (Other related but secondary recommendations are excluded from this table, but are available at <a href="http://www.sec.gov">www.sec.gov</a>.)</p>		

## **COST & BENEFIT CONSIDERATIONS**

The PCAOB strives to determine that its standards meet a significant need and that the costs they impose – compared with possible alternatives – are justified in relation to long-term benefits. When a new activity or responsibility requires an initial investment in new audit programs and training, then any increase in fees is likely to be larger during this period, before ultimately reaching a stable state. Moreover, when the learning period is necessarily condensed (due to external reasons such as legal deadlines) the audit resources required to fulfill the new obligation also generally increase to reflect the expedited nature of the undertaking. Lastly, when companies are also required to undertake parallel new activity during this same time period, and both auditors and their clients are learning simultaneously, the overall start-up costs of the new activity will be larger still.

This is the factual scenario that presented itself to US-accelerated filers and their independent auditors in 2004 and early 2005 – the first year of implementing §404. Studies calculating these first year costs do not always use the same means of measure, but most agree that the average per-company cost was approximately \$4.36 million (with approximately \$1.34 million paying for internal company resources, \$1.30 million going to outside auditors, and \$1.72 million being used for external costs such as consultants and software). Three points, however, are relatively undisputed:

1. Year 1 costs disproportionately affected (as a percentage of revenue) smaller accelerated filers. Since a substantial component of auditors' annual fees are "fixed" (i.e., represent mandatory activity that must be performed each year), this is also generally true of the costs of financial statement audits. Whether, and if so how, the same degree of impact will occur for small companies that have not yet implemented ICFR requirements remains unknown, although it is a matter of considerable debate (see pages 7-8, above).
2. Year 1 ICFR costs far exceeded the SEC's (and probably Congress') initial expectation. The key reason for this mismatch between expectations and reality is the discovery that prior to the enactment of §404 and despite the existence of the Foreign Corrupt Practices Act, ICFR was not a high priority of either companies or their auditors. As a result, much of the first year costs (over and above the "learning curve" costs discussed above) were the direct result of documenting ICFR systems and correcting ICFR flaws that had long existed – the so-called "deferred maintenance" costs.

3. Average Year 2 costs (including both auditor's fees and company costs) of ICFR are expected to decrease. This is a natural result of the end of Year 1's learning curve, as well as an outcome of significant additional guidance provided by both the SEC and PCAOB during the past 12 months.

While §404 costs are relatively quantifiable, its benefits are not. What is the value of increasing the reliability of the financial numbers upon which the markets move, and individual investment decisions are made? When enacting the Act, Congress made a determination that increased reliability has an inherent value – not only to investors, but also to company employees, the community, and the national economy. A number of factors, some of which are subject to quantitative analysis and others that are not, are relevant; e.g.,

- *Does the **auditor's** independent assessment of ICFR make a difference?* At least one analyst noted that as the deadline for auditor reports approached, “reported control deficiencies rose significantly even though many CEOs and CFOs had reported earlier – under the requirements of §302 certifications – that their internal controls were effective.” (See Glass Lewis & Co., June 24, 2005.)
- *What do those within a company who are closest to ICFR (and have gone through the process) think?* The reactions are mixed. In a January 2006 poll conducted by CFO Magazine, 24% of the 237 respondents said that §404 is the one provision of the Act *least* beneficial to shareholders. Thirty-five percent, however, said §404 was the Act's *most* beneficial provision to shareholders. In an April 2005 survey by Oversight Systems, Inc., 50% of the financial executives queried said that compliance with the Act reduced the risk of fraud and errors; 48% said that, because of the Act, they now have more efficient financial operations. Similarly, in a January 2005 survey by the Institute of Internal Auditors Research Foundation, over 60% of the 171 responses from chief audit executives agreed that there have been improvements in their companies' control environments, as well as anti-fraud awareness activities, that would *not* have occurred *but for* §404.
- *Has increased regulation arising from the Act impacted the ability of private equity to access the public markets?* In March of 2006, SME Capital Markets published a report demonstrating that in 2005 the number of small companies filing with the SEC to be public reached a record 881. (Filings were 800 in 2004, and 435 in 2003.)

- *Does increased reliability in financial information affect a company's cost of capital?* In a soon-to-be published study, the researchers conclude that the median increase in the cost of equity that occurs when a company is judged not to have had reliable audits is almost 50 basis points. (See Kinney, Botosen and Palmrose, *The Value of Financial Statement Audits: Do Benefits Exceed Costs?* (Synopsis of work in progress, May 19, 2005).)

Many of the studies identified above, as well as those expected in the future, all seek to identify benefits or harm to shareholders. In the end, however, it is really only those shareholders who can decide whether the advantages of the ICFR requirements outweigh the costs.

## OPPORTUNITIES FOR INPUT

- To provide the SEC with comments regarding ICFR prior to the May 10, 2006 roundtable, go to <http://www.sec.gov/news/press.shtml>, and look for Release No. 2006-34. This will take you to an electronic comment box. Or, send written submissions in triplicate to:

Nancy M. Morris, Secretary  
Securities and Exchange Commission  
100 F Street, NE  
Washington, DC 20549-1090

All submissions should refer to File Number 4-511.

- To provide the PCAOB with comments regarding ICFR prior to the May 10, 2006 roundtable, go to [http://www.pcaobus.org/News/Releases/Pages/02162006\\_PCAOBandSECRoundtable.aspx](http://www.pcaobus.org/News/Releases/Pages/02162006_PCAOBandSECRoundtable.aspx), and look for the Comment Link. This will take you to an electronic comment box. Or, send written submissions to:

Public Company Accounting Oversight Board  
Attention: Office of the Secretary  
1666 K Street NW  
Washington, DC 20006-2803

Refer to "Internal Control Roundtable."

- To provide comment on the SEC's Advisory Committee on Smaller Public Companies, go to <http://www.sec.gov/rules/other/33-8666.pdf>. Refer to File No. 265-23. **The deadline for comment submission is April 3, 2006.**

**PLACES TO GO FOR MORE INFORMATION**

SEC Web site: <http://www.sec.gov/spotlight/soxcomp.htm>

PCAOB Web site:

[http://www.pcaobus.org/Standards/Auditing/Pages/Auditing\\_Standard\\_2.aspx](http://www.pcaobus.org/Standards/Auditing/Pages/Auditing_Standard_2.aspx).

## NOTES

## APPENDIX

## APPENDIX A-1

### **Section 404 of the Sarbanes-Oxley Act of 2002 (the Act) states that:**

(a) Rules Required.—The Commission shall prescribe rules requiring each annual report required by section 13(a) or 15(d) of the Securities Exchange Act of 1934 (*15 U.S.C. 78m or 78o(d)*) to contain an internal control report, which shall—

(1) state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and

(2) contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.

(b) Internal Control Evaluation and Reporting.—With respect to the internal control assessment required by subsection (a), each registered public accounting firm that prepares or issues the audit report for the issuer shall attest to, and report on, the assessment made by the management of the issuer. An attestation made under this subsection shall be made in accordance with standards for attestation engagements issues or adopted by the Board. Any such attestation shall not be the subject of a separate engagement.

**APPENDIX A-2**

**Section 103 of the Act states (in part) that:**

(a) Auditing, Quality Control, and Ethics Standards.—

(1) In general.—The [PCAOB] shall, by rule, establish . . . such auditing and related attestation standards . . . to be used by registered public accounting firms in the preparation and issues of audit reports. . .

(2) Rule requirements.—In carrying out paragraph (1), the [PCAOB]—

(A) shall include in the auditing standards that it adopts, requirements that each registered public accounting firm shall—

(i) . . .

(ii) . . .

(iii) describe in each audit report the scope of the auditor's testing of the internal control structure and procedures of the issuer, required by section 404(b), and present (in such report or in a separate report)—

(I) the findings of the auditor from such testing;

(II) an evaluation of whether such internal control structure and procedures—

(aa) include maintenance of records that in reasonable detail accurately and fairly reflect the transactions and dispositions of the assets of the issuer;

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

(III) a description, at a minimum, of material weaknesses in such internal controls, and of any material noncompliance found on the basis of such testing.

.....