James J. Angel, Ph.D., CFA
Associate Professor of Finance
McDonough School of Business
Georgetown University
Room G4 Old North
Washington DC 20057
angelj@georgetown.edu
1.202.687.3765

Ms. Nancy M. Morris, Secretary
Securities and Exchange Commission
100 F St. NW
Washington, DC 20549-9303
Rule-comments@sec.gov

Office of the Secretary
Public Company Accounting Oversight Board
1666 K St. NW
Washington DC 20006-2803
comments@pcaobus.org

February 26, 2007

File No. S7-24-06: Management's Report on Internal Control over Financial Reporting
PCAOB Docket Matter No. 021

Here are my comments on the proposed "guidance" and rule changes. In brief:

- The implementation of §404 by the Commission, the PCAOB, the accounting profession, and issuers resulted in *de facto* regulatory requirements far beyond the requirements of the text of the statute.
- §404 was in keeping with the basic philosophy of U.S. regulation: disclosure. §404 should be interpreted as a disclosure requirement of the current state of the issuer's internal controls, not as a dictate for any particular level of controls or control verification.
- The resulting implementations of §404 have generally assessed control effectiveness in black-and-white terms: either effective ineffective. This provides little useful information to investors.
- The proposed SEC guidance does little to fix the regulatory train wreck that occurred in the implementation of §404, and indeed only compounds the problem with its vague "guidance" that lack clear examples of a realistic safe harbor.
- Rather than a binary black-and-white standard, the assessment should disclose the level of the quality of controls. For example, internal controls could be graded according to different frameworks, similar to credit ratings. Issuers would then

choose whether it is cost effective to spend the resources to earn a AAA internal control rating, or whether a single A is good enough.

- The proposed new auditing standard is a step forward, but does not fix the original mistake in the implementation of §404: a binary assessment of effectiveness rather than real disclosure of the current level of internal controls.

Background

The SEC, PCAOB, and Congress have been inundated with howls of protest over the implementation of §404 of the Sarbanes-Oxley Act of 2002 ("Sarbanes-Oxley"). The "overly conservative" (in the SEC's phrase) implementation has resulted in a massive increase in auditing costs for public companies in the United States. Many feel that the time and expense of the exercise will not do much to decrease the probability of another Enron or WorldCom level fraud. No wonder, then, that many firms have chosen to deregister their securities and exit the public capital markets of the United States.

How did this regulatory train wreck happen?

In the wake of Enron and WorldCom, Congress passed Sarbanes-Oxley. Among other things, the act created the Public Company Accounting Oversight Board (PCAOB), increased penalties for financial fraud, tightened standards for corporate governance, increased requirements for auditor independence, and increased the SEC budget. In particular, Title IV, Enhanced Financial Disclosures, called for more disclosure of transactions involving management and principal stockholders, disclosure of the existence of an audit committee financial expert, and disclosure of a management assessment of internal controls.

The Commission and the new PCAOB duly passed a number of rules to implement Sarbanes-Oxley, and issuers set about to comply. Alas, the rules for §404 generally called for a binary assessment of whether or not controls were "effective." This was the key mistake. Internal financial controls are basically a risk management exercise. How much money should the company spend to set up procedures to prevent materially bad things from happening? What should be the cutoff probability that something "material" could happen? And how big is "material", anyway? Which controls are "key"? A lot of the contentious issues come from these judgment questions about how much risk is acceptable.

It is downright silly to think of risk management in black-and-white terms. One can always argue that a particular cut-off level for an acceptable risk is too lax or overly conservative. It comes down in the end to a matter of judgment. (Indeed, I notice that the word "judgment" appears to be used 31 times in the SEC's proposing release.)

It is usually impossible to remove all risk. Even if it were technically possible, it would be so expensive as to be impractical. For example, one could protect a single vending machine by installing a Fort Knox-like security system with cameras, sensors, and armed guards. But the cost of doing so would be more then the revenue from the vending machine. Individuals, businesses, and governments every day make risk management decisions in which they accept some risk because the costs of additional risk reduction are not worth the benefits.

The auditors, recently chastened by the public execution of Arthur Andersen, generally required expensive procedures to document and test internal controls before they would attest to management's evaluation that the controls were "effective." And who can blame them? If they required an overabundance of paperwork to cover their backsides, they were just doing their job. On the other hand, if they only required the socially optimal amount of paperwork (the point at which the total costs to society equaled the benefits), there would still be some risk, however small. If that tiny bit of risk blew up in a particular situation, then the auditor involved would be in deep trouble. Given these professional incentives, the auditors did the natural thing and performed an "overly conservative" -- and overly expensive – implementation of §404.

Issuers were caught between a rock and a hard place. Even if it made no economic sense to do what the auditors demanded, issuers were forced to comply or else they would get a "failing" grade from the auditors. No issuer could dare let "ineffective" grades go uncorrected, even when it made no economic sense, because of the potential legal liability if something happened and their "ineffective" controls were blamed.

Issuers were thus stuck with doing whatever the risk-averse auditors said to do, resulting in massive compliance costs. The general consensus is that the costs exceed the benefits. The Financial Executives Institute survey found that 85.1% of surveyed firms believed that the costs of 404 compliance exceeded the benefits.[1] The survey also found that the average large company (market capitalization over $700 million) spends over $5 million per year on §404 compliance.[2] This implies that the total amount spent on Section 404 compliance is more than the total budgets of the SEC and PCAOB combined.

What should be done about it?

§404 was basically a call for better disclosure. Its placement in Title IV, *Enhanced Financial Disclosures*, was no accident. Note that this title was not named *Enhanced Auditing Requirements* or *Enhanced Control Requirements*. Title IV fits in with the long tradition of U.S. financial regulation to promote disclosure and transparency in the markets.

[1] FEI Survey on Sarbanes Oxley § 404 Implementation March 2006. http://www2.fei.org/files/spacer.cfm?file_id=2104

It is useful to recall the actual wording of the law:

SEC. 404. MANAGEMENT ASSESSMENT OF INTERNAL CONTROLS.

(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.

Note that §404 calls for "an assessment … of the effectiveness … " It does not call for specific controls or procedures. Congress was basically calling for more information, just as it was with the other requirements of Title IV. However, the black-and-white disclosures that have resulted from the implementation provide investors with little information. If the controls have been deemed "effective," the 10-Ks just contain standard boilerplate that the controls are "effective." If "material weaknesses" have been found, then there is a tiny bit more information about the nature of the weakness.

As a professor, I do assessments of my students frequently. Most of the time, the assessments are more than just pass/fail. Instead, they range from A to F. In financial services, credit rating agencies also assess the risk of various debt offerings. These evaluations provide important information that permits investors to make intelligent investment decisions.

There are over 10,000 public companies in the United States. It does not make sense for all of them to have the same types of internal controls, or adopt the same framework for assessment of those controls.

One possible evaluation would be for there to be different acceptable frameworks for assessing the effectiveness of controls. These different frameworks would have different definitions for items such as "key control," "material," "significant," "reasonable possibility," and "effective." They would require different levels of documentation, different levels of testing, and permit different levels of reliance upon previous years' audits. These different frameworks could be graded as AAA, AA, A, etc. just like credit ratings.

Instead of merely opining that controls were "effective," management could state that its controls were effective under a particular standard that was one of a menu of acceptable standards. Just as investors decide whether a single A rated bond is good enough for their portfolios, they could decide whether a firm with single A rate controls is good enough as well.

Management already has the correct financial incentives for most internal financial controls. If the controls break down, the financial impact on the company directly affects management. Managements should have the flexibility to choose which level of controls and which levels of controls assessment are most cost effective for their companies.

The only area in which top management does not have the correct incentives is one in which top management itself is involved in a fraud such as in Enron and WorldCom. This implies that the emphasis of the 404 audit should be on those top-level controls that would serve as a deterrent to fraud by top management. To this extent, the emphasis in the PCAOB's new auditing standard on a top-down approach is a step forward.

In terms of scalability, the proposed auditing standard is still somewhat vague. Given the understandably risk averse nature of the auditors, it is not likely that they will suitably scale down their requirements for smaller firms. By allowing a number of different acceptable frameworks, the responsibility will be on management rather than the auditors to select the appropriate framework. This reduces risk for the auditors, and also will lead to a more cost effective level of expenditures on §404 compliance.

Congress left it up to the SEC and the PCAOB to use professional judgment in writing the rules for §404 implementation. I call upon the SEC and PCAOB to use this discretion to fix the basic flaw in the original implementation of §404, the black-and-white definition of "effectiveness," and to come up with a common sense menu of acceptable assessment frameworks that will implement §404 in an efficient manner.

Respectfully submitted,

James J. Angel, Ph.D., CFA