To: The Securities and Exchange Commission
From: Kirke Bent
Parallel Business Software
Chatham, NJ
On: Concept Release Concerning Management's Report on Internal Control Over Financial Reporting

Support for Sarbanes-Oxley

I fully support this law and the SEC's work enforcing it. I hope that the SEC will issue further rules and recommend further legislation if it turns out that more is needed to reduce fraud. The climate at the top is important, and the branches of government are certainly part of the top.

The approach of helping corporations to implement requirements, rather than watering down requirements, is a good one. Why?

a) The 2006 ACFE Report of fraud points out that "Small businesses continue to suffer disproportionate fraud losses."
b) Reduced requirements for smaller corporations would inevitably lead to strong pressure to reduce the requirements for larger ones, even assuming that the law permits different levels. In this connection, it should be noted that the June 2006 COSO *Guidance for Smaller Companies* says that the Guidance can be used by companies of any size.

If it is necessary to define a lower level of compliance, this should not be rationalized in any way that undercuts the "professional skepticism" of good auditors. For example, justification should not be that some class of managers is more or less trustworthy than another or knows their business better than another.

Informing Investors

When certain corporations are permitted to delay compliance or even comply at a lower level, this fact should be clearly indicated in filings and in communications to audit committees, regulators, and investors. Officers' formal reports should positively and explicitly report and certify that internal controls are NOT certified at the best level or NOT certified at all because of a deadline extension. Auditors should certify the same thing.

This would have the very important advantage of fuller disclosure to investors, and would also confer a further benefit to corporations that do comply at the highest level and comply as soon as possible.

Employee Investors

When a tax-privileged defined-contribution retirement plan calls for investment in the corporation's own stock, including most especially 401(k) plans, the corporation should be given no latitude concerning immediate compliance at the highest level.

Since the Pension Protection Act of 2006 permits automatic enrollment, we can expect to see many investors who are not sophisticated and who are not protected by an intermediary such as a mutual fund.

The existence of fiduciary obligations does not reduce the need for controls and certification. Errors and fraud are always possible. The case of a well-known corporation was reported in the New York Times earlier this year. The corporation had to restore millions of dollars to an employee pension plan because legal and actuarial expenses for a non-qualified plan for management had been charged to the employee plan. The tax status of the original payments was likely incorrect.

IT

Since IT is so pervasive and powerful, control of IT processes should be certified just as any other. Of course, the nature of controls may differ. The comments in this section are general. They are expanded on and made more specific below, using the vulnerable financial close process as an example.

The scope of IT controls should be appropriately broad. By any good definition of programming, the large commercial ERP systems are **programmed** by the settings in thousands of tables. Since these settings constitute a program, they should be subject to the full range of IT controls, both company or entity-level and account-specific. There should be no presumption that the tables have not been modified since installation or since the last major upgrade, since this is highly unlikely.

The same applies to spreadsheet and database/reporting systems. These are sometimes considered as “user” systems, but they are fully programmable and extremely powerful. Where they are used to calculate values that affect statements, they should be subject to the full range of IT controls. Examples of such use are cost allocations and depreciation schedules. Otherwise, there is no good defense against errors and manipulation.

COSO Guidance for Smaller Companies

It would be very easy to make an incorrect inference from the June 2006 COSO *Guidance for Smaller Companies*. While you probably do not want to comment specifically on any framework, it would be valuable if the SEC guidance cautioned companies to avoid making comfortable but incorrect choices. This is especially true since on page 1 volume I the document says that it is intended for smaller companies but is “usable by large ones “.

First, the COSO document identifies a lesser level of IT controls needed for less complex IT environments. It suggests that minimal change control is necessary between major upgrades of ERP software. The idea is that ERP software is different than in-house developed software because changes are made by the vendor. There isn’t a stream of patches and changes that might (or might not) be expected with in-house developed software.

This misses a significant difference between in-house and packaged software. Since packaged ERP systems are developed for use by many companies, of different sizes and in many different businesses and jurisdictions, they are extremely configurable, having thousands or tens of thousands of tables. Configuring changes the software from a potential application to an actual one. The same needs and pressures that result in changes to in-house developed software can be expected to apply to the programming of a packaged ERP system via configuration parameters.

The last section of the last volume has a number of very good criteria for a less complex environment, including this one: “User-configurable options do not significantly alter the functioning of the application”. I suggest that this is a rare circumstance.

Second, spreadsheets are characterized as End User Computing. The criteria for a less complex environment do not mention spreadsheets. A better way would be to classify spreadsheets according to whether or not they produce results that affect financial statement figures. If so, they should be subject to IT controls.

The last page of the last volume has a treatment of spreadsheets that is good, as far as it goes. It reflects a degree of idealism that should be an example to us all. It deals with various ways of avoiding inadvertent errors, primarily dealing with access and protecting input data. There are two problems that need to be dealt with before assuming that spreadsheets are safe in smaller companies.

First, the control concepts described in the COSO documents are precisely the things people want to avoid when they go to end user computing. It is unrealistic to think that those controls would be used in the period close process, for example.

Second, while the control concepts can be helpful in preventing inadvertent errors, they provide little if any protection against fraudulent manipulation. This is because spreadsheets are different than conventional programs in an important way. We can use the term “base spreadsheet” for spreadsheets with logic and input data well protected. However well protected a base spreadsheet is, when that base spreadsheet is used, it is always possible to create new “sheets” within the spreadsheet to look like the protected ones. Data can be brought forward to where it can be changed readily. The same applies to formulas. Spreadsheets are a serious hazard. The popular term “spreadsheet Hell” doesn’t come from nowhere.

Financial Close

The financial close process is vulnerable to error and fraud. Fraud because that’s when it becomes clear how much false earnings would be needed to match earnings goals. Error prone because financial close processes have significant manual components, including spreadsheets, and are not repetitive. When that is added to time pressure, the financial close is clearly exposed.

Assume a hurried and harried financial close process and then consider a process such as cost allocation. As an example of potential problems, cost allocation can be used fraudulently to move cost from a current category to one that goes into the income statement very slowly. There are numerous examples of actual fraud committed by cost misclassification.

When allocations are calculated with a spreadsheet, the same person might very well: prepare the specifications; do the programming; do the testing; safeguard the program; supply the input data; operate the program; use the results; and protect the results.

Segregation of duties would be absent, as would all IT controls. If a number of alternate calculations are tried, the last version of a spreadsheet may very well not be the version that was actually used. The auditor's ability to repeat the calculation is compromised because of this and because we cannot expect that spreadsheets are protected. The actual process would not be adequately documented. If there is an assessment of controls on these processes, the evidence can be expected to be scanty or nonexistent.

How could this hypothetical process be considered controlled? It couldn't. I suggest that spreadsheets are used for substantial parts of the close process for most corporations, and that IT controls and segregation of duties are incomplete at best.

Allocations are vulnerable even when done with the facilities of an ERP system. Allocation rules can be changed, executed, and then changed back. The changes might very well be logged but unless careful and pointed use was made of the logs, such changes are unlikely to be detected. Further, segregation of duties can readily be compromised at financial close because of time pressures.

Finally, last minute adjustments are a hazard. They may not be calculated using tested procedures. They might be used for fraudulent purposes. They contribute to a poor climate where high-level people are making poorly understood changes outside of normal procedures and controls, setting a bad example.

According to expert witness testimony at the Enron trial, every company does last minute adjustments. Note: **"every"** company. It is not necessary to take this literally to believe that such adjustments are common. The existence of such adjustments can be taken as evidence of failures of processes, especially computerized procedures. Among other things, IT controls should focus on these adjustments, with an eye towards correcting the underlying causes.

All this is offered to support the idea that IT controls need the full attention of management, and should be assessed and reported on along with other controls. Companies should not make comfortable assumptions about the need for controls unless those assumptions are fully justified.

Use of Software Packages

Software packages can be a big help. Subject to cost/benefit determination, they should be used. The same caution should apply to them as applies to check lists, frameworks, consultants' advice, etc.: relying on any of these is not a substitute for management's responsibility to make sure controls are adequate.

Thank you for the opportunity to make these comments.

Kirke Bent
September 1, 2006