August 3, 2006

Release No. 34-54122; File No. S7-11-06, RIN 3235-AJ58

Mr. Chairman and Honorable Commissioners:
The SEC is soliciting comments to help itself understand the extent and nature of public interest regarding the task of evaluating and assessing internal control over financial reporting. The SEC states the goal of this solicitation is to "address the needs and concerns of public companies, consistent with the protection of investors." This is submitted to support reaching the *protection* objective.

Commentary is also being provided on the subtask of "evaluation and assessment" – the intermediate SEC target. The level of interest represented by this Professional Engineer (PE) and veteran internal audit/control practitioner (IIA), thereby, speaks for itself. The conditions of my license call for fealty to the stakeholders of design equal to your Congressional mandate to protect the investors – no more and no less. The PE standard of care has placed stakeholder protection "paramount" for more than a century. No other discipline responding to this solicitation, including law and accounting, is burdened with the obligation to protect the public at large. PEs cannot consider standard regulatory response to corruption and fraud, where the damage already inflicted on the stakeholders will be born by the stakeholders, to be in any manner contributory to the "*protection* of investors" goal. On the contrary.

Overview
Like it or not, the stated task, "evaluation and assessment," is an integral part of the basic system design cycle engineers call run, break and fix (RBF). In practice, procedures for evaluation are amalgamated with testing for operating effectiveness. Designing the amalgam requires absolutely objective benchmarking first. The effort to nail the non-subjective standard for effectiveness, in fact, occupies most of the total task. The concern of "reasonable evidential matter" evaporates during the struggle to keep internal control viable and should be abandoned. The appropriate method is inherently data and documentation intensive. The documentation of inappropriate methods, always done by backfit, is worthless.

Generic abstract evaluation frameworks peppered with judgment - don't work (II.3). There are sound reasons why, for matters in the future, subjectivity is a loser. The most gifted of designers is embarrassed by the track record of his guesswork concerning system dynamics in possible futures. Savvy designers never guess futures they can investigate (model) and, now, any specific future can be computed. Judgment cannot be completely removed from hindsight practices and interpretations of history, but it has no place substituting for the dynamics of specific futures that can be reliably calculated to specified levels of confidence. All benchmarks for effectiveness are local, scenario by scenario.

There can be no process of design (evaluation and assessment) without RBF. You imagine a candidate configuration, take it over the proving ground, find out it doesn't perform as you had guessed, and invent another configuration. Repeat as necessary. Evaluate and assessment cannot be treated in isolation as a stand alone analytical procedure, like carbon dating. So, when the SEC thinks assessment, it neglects the institutional proving ground that must have been used repeatedly to arrive at the internal audit/control design in the first place. The bone of contention you encountered is really between the proving ground design you think you want annually and the one already in service that management thinks it wants – today.

The submittal format follows the flow of standard PE goal-seeking project practice. This is part one – Congruent Objectives. Part two will apply engineering principles to evaluate the approach being used by the SEC for consistency with natural law in seeking its stated goals. Part three will review the irrevocable requisites of attaining the stated goal, highlighting the difference between the PE standard of care and business as usual at the SEC. The SEC will do itself a great favor by recognizing the fact that the certainty of outcomes is driven by natural laws – and has nothing at all to do with the cast of players, their ethics, and their qualifications, as your history attests. If you insist on devoting your energies and resources to

continuing attempts at defying natural law, as you recently did with pay disclosure rules, your future, like that of your investors, is unprotectable.

The numbers in parentheses attending the comments reference the itemized SEC issues in the concept release.

Congruent Objectives

Alexander the Great was one of a long line of militants that initialized impending engagements with a side trip to the Oracle. Don't bother to embark until you have independently validated your plan to attain the goal, is a tradition acquired the hard way. The SEC routinely skips this visit to Delphi. The first step in any engineering project not engaged in replication is to determine, in algorithm form, that the chosen scope and methodology hide no attempt to defy natural law. This step cannot tell you what course to take any more than the stoned lady perched on the three-legged stool. The oracle of natural law only flags practices that will be counterproductive for the particular mission in hand.

In the critical matter of goals, one must wonder why the SEC red-flags that protection of investors is inconsistent with "the needs and concerns of public companies." The top pay fiasco has made it plain what management actually does. It is abundantly clear who stands to gain and who loses when you don't attain your stated goal. External auditors have understood and aligned with the actual goals of management from the inception of the discipline in Medieval Venice. That's where the money is.

Characteristics of SEC's composite manager

Your concept release reveals the manager composite you use as reference to shape your concerns. Make no mistake, composite manager already has, exactly, the internal audit/control system he thinks he wants today. He has had an evaluation and assessment system in place from the outset, which is how he derived his design. The SEC thinks that management needs "guidance" to comply with the stated regulatory intent for the following stated reasons.

1 – It lacks a "suitable evaluation framework" (IV.22)

2 – It lacks procedures to scope and evaluate its design by measures of operating effectiveness (IV.24).

3 – It fails to bring "reasoned judgment" to the compliance process. (May 16, 2005 guidance)

4 – It fails to recognize, classify and respond appropriately to institutional risks, especially fraud (II.11, II.14)).

5 – It fails to account for events that drive change to the "nature, timing and extent of its evaluation procedures," (IV.23).

6 – It has no stop rules for aligning the severity of risk with the strength of internal controls (III.19).

7 – It has no benchmarks for distinguishing material weakness or significant deficiency (II.12, III.18, IV.26 & 27, V.25).

8 – It does not collect and organize operational data consistent with the stated SEC mandate to provide documentation assuring that stakeholders are protected (V.31, 32, 33, 34).

The composite manager fails to rationally evaluate his internal audit/control system by your benchmarks because he has no use for your objectives in the first place. The SEC composite manager does not support risk-informed decision-making to run the institution. The management that displays such brilliance in surreptitiously rewarding itself to stratospheric levels and the knowledge-challenged management seemingly

unable to design and evaluate his internal audit/control system for regulatory compliance are one and the same. If management used the information requisite to meet the stated SEC intent in leading the institution, there would be no stakeholder damage crisis demanding SEC attention.

You think that once management is informed of SEC-provided compliance guidance, everything will turn out OK. Replace that assumption with one that finds management going to great lengths to maintain his internal audit/system producing that which he wants, today, no matter what disturbance arrives from the SEC. If you feel you have to advise management how to implement and assess such a fundamental process requisite to the firm's survival, you should also advise the stakeholders to rid themselves of the menace to their future.

The operational goals of management have been brightly illuminated by the SEC initiative concerning head shed remuneration. The unprecedented response to the SEC solicitation of stakeholder commentary speaks for itself. When you made it the responsibility of management to determine the appropriate nature and form of internal controls, you endorsed management's license to print money. Management's internal audit/control system is there to attain management goals. The two matters are bound together in the institutional setting. The PE must combine the lessons from 404 and pay into one coherent knowledge base. It is impossible, for instance, to align the internal audit/control system to stakeholder *protection* and not automatically remedy the head shed remuneration issue. Management does not separate these matters. Why does the SEC?

Clearly, SEC goals (as stated) are in a code/decode relationship with head shed aims and it is adversarial. The regulatory system, of which the SEC is a part, insists on attaching responsibility for protecting stakeholders to the CEO and grants him dictatorial powers to do so. CEOs are not licensed professionals. They are duty bound to no standard of care but the one they choose for themselves. To the stakeholders, the SEC portrays its relationship with the people directly responsible for stakeholder damage as congruent. Since the brute facts show the actual regulatory relationship as code/decode, the head shed has the overwhelming advantage to achieve its goals at the cost of whomever it may concern. The advantage deliberately transferred to management, for example, allows the executive chicanery with stock options to flourish for years "undetected" by the watchdogs commissioned by Congress. If Congress were to look, it would find the SEC was first notified about the devious option practices via informers ten years ago or more.

While the SEC, by habit, is handling the matter of internal control/audit by 404 as a joint affair of responsible management and the SEC, the PE can afford no such luxurious assumption. The recent SEC amendment concerning pay disclosure is a chilling example of giving the adversary your latest code so to make his decode (loophole) task easier. Of course the SEC knows it can't collude with the incongruent goals of the regulated and protect the stakeholders at the same time. The SEC also cannot conceal which choice it is making. The purpose of the system is what it does (POSIWID). The pileup of stakeholder damage, now accumulating faster than the SEC can prosecute cases, speaks to the stakeholders directly. The problem the SEC has is that unless the stakeholder wreckage abates, SEC business as usual will propagate instability in all directions. To the PE, it takes more than sharing the same stated goals to assist the SEC. The methodology appropriate to the goals shared must be congruent as well.

Congruency first

Every PE knows that all significant projects that fail, do so at the outset. The reason is always mismatch of methods chosen to the attributes of the goal. It is a simple matter to detect a mismatch, without error, upfront before the debacle commences. The Big Dig in Boston, for example, was known by participating PEs to be a certain calamity from the beginning of the project twenty years ago. Within a month after kickoff everyone knew.

The congruency test checks for two kinds of error. First is to make certain that the goal stated aligns with what is needed. Alignment occurs so rarely you can take it for granted that the stated goal is far askew from

the goal that will deliver the future desired. What happens in practice is that the real project goal becomes a bastard mix offending everyone. The second error field is a mismatch of methodology chosen to the requisites to reach the goal. What happens in practice is that the working environment established by the institution will only support one methodology – obedience to authority (rules of action). If the project entails novelty or encounters novel disturbances, it locks into the black hole of perpetual crisis mode. Truth be known, the SEC is not now far from the event horizon.

The PE defines his duty to protect stakeholders paramount in terms of foresight, not hindsight. The trail of stakeholder damage only attests to requisite PE due diligence; it does not trigger action. To the PE habit of thinking, the SEC policy of responding to de facto scandal and fraud (hindsight), no matter how brilliant and forceful, exhibits an intrinsic failure to protect – especially since few stakeholders ever see anything but token damage compensation. It's one thing to fall short on preventing scandal, but quite another to be making corruption easier to arrange.

Goal context

Intrinsically, stakeholder protection is a moving target locked to the future, publicly graded by history, with contemporaneous assurance of attainment a lawful duty. Everything related to providing protection rolls forward with the clock. Designer heads must be in the future, the only place that protection can be attained. This exercise of foreseeability must meet the standard of care – a methodology and technology that is rapidly advancing – in the immediate present as the project moves ahead. The whole arena is far too dynamic for a rules-based approach. The half life of a SEC rule of action today is measured in months.

The professional requisite is that when the record does not improve by your practices, you must change your practices – and make sure your RBF cycle time is appropriate to the challenge dynamics. The biannual measure of watchdog regulatory effectiveness concerning fraud, published by the ACFE, is an incontrovertible measure. The sophisticated 2006 report is available to the public. The data show occupational fraud is increasing with time across the board. The utility function of annual benchmarking evaporated years ago when the pace of fraud and scandal accelerated. If the trend continues, fraud will soon be a trillion dollar a year "business." The report steers clear of regulatory accountability for the unmitigated growth in corruption and no regulator steps forward to claim responsibility. Telling.

The fact that all fraud, corruption and scandal will never be eradicated has nothing to do with the huge benefits of intelligent prevention practice. Both contenders are viable systems in a code-decode embrace. Fraudsters will try new assaults and we will continue to improve our methods of prevention (transparency). We both will leverage technology to meet our aims. The report card of effectiveness for society is provided by history.

Engineering definition of Stakeholder Protection

As indicated above, our working definition must provide assurance, as we go, that the future will affirm best foreseeability practices were used competently and contemporaneously to protect stakeholders' future – specifically from fraud, misleading reports, and cooked books. To the PE, this requisite is the standard duty of design. The only way to assure ourselves as we go of meeting due diligence is through quantitative measures of "foreseeability." Thanks to enormous advances in foreseeability technology enabled by huge computational power, methods are now available to the PE for attaining stakeholder protection without the use of subjective benchmarks.

When we protect the stakeholder, we protect ourselves. Subjective benchmarks always involve the risk of retroactive second-guessing by non-engineering disciplines in authority. The definition of "reasonable person/assurance" has a tendency to creep with the "dynamic and evolving nature of business" and whims of the legal system. The gold standard of stakeholder protection is transparency. As a famous judge once observed, "Sunshine is the best disinfectant."

As the future is where protection occurs, that's where your design knowledge must reverberate. History is always an input, of course, but the PE knows the actual trail of the past is just as unlikely as any exact path the future will take – and both are far less likely than guessing the lottery. What we do is use natural law to arrange a transfer function, an algorithm, to drive us in steps from state A (known) forward to a state B, computed, that otherwise would rely on guesswork. This makes the foresight reliable and transparent (engineering foresight) scenario by scenario. There is no prognostication of the actual future in engineering foresight. The opportunities are investigated one specific pathway in the possible future at a time.

The rolling outcome forecast is within tolerance to the rolling actual and prepared with reliable, timely knowables about institutional performance and prospects. Stakeholders are deemed protected when they are provided with data, necessary and sufficient, compiled from the data used to forecast the future by the institution, which can be composed by the stakeholder to futurecast with stated levels of confidence. The use of quantitative measures, produced by an algorithm also available to stakeholders, is the subjectivity-free contemporaneous compliance sought by the PE. This definition is easier done than said.

Compliance Checklists

SEC officials often bemoan the observed checklist mentality of the regulated in their public speeches. The dominant syntax of commissioner encounters is the checklist of task actions comprising, in the aggregate, compliance. Somehow, the brute fact that regulating by rules of action engenders the check-the-box response is never discussed. You can have rules of action or you can have attainment of your objectives. Natural law forbids you from having both together.

As protection of stakeholders/investors is the specification at the apex, allow for the fact that protection success can only be measured in the future. Once history develops, ongoing protection practice has no influence on the record past. Protection, prevention, avoidance, anticipation and preemption are all forward looking procedures. Unfortunately, the difference between regulation by rules and regulation by goals is methods of compliance that are mutually exclusive. The code/decode relationship can only exist when regulation is by rules of action.

The methodological realm that defines an institution, any institution, is limited to hindsight and emergency response. The only compliance practice compatible with hindsight and crisis response is obedience to authority – where SEC rules of action comprise the authority to be obeyed – or bypassed. The signature of this orientation to compliance is the task checklist. To the regulated, the checklist equals compliance. The aims and purposes of compliance and the stakeholder wreckage that results remain the responsibility of the regulator, since ends responsibility was never transferred to the regulated, just means.

As long as you insist upon regulation by rules of action, you will retain responsibility, alone, for stakeholder damage. You will not attain your stated goal of protection until you transfer responsibility for the attainment of protection to the regulated – exactly like the PE standard of care. Once glued to goals, the regulated must be set adrift to use whatever actions it finds are effective at the time. Since protection is a foresight matter, the regulated have to be as free as any designer to engage trial and error, suck and see, and RBF. If management does not then use the data engineering foresight compels it to develop for running the company, as the stakeholders can see for themselves, the regulatory intent is not sustainable.

You think you can get into the details of compliance practices under the guise of "guidance" and stop short of issuing a checklist of compliance practices. Once the regulated get their authorized checklist for compliance, all concern about goals, objectives and responsibility to stakeholders is immediately displaced by obedience to the list (II.7). There is no stopping point from stating goals to attaining goals. Your audience will harass you for guidance until they get the blessed checklist

For the stated purpose of protecting investors through foresight transparency, rules of compliance lead to a dead end. Providing detailed guidance for rule compliance is a tar baby. It is easy to fall into the trap of

drill-down guidance and impossible to get out. In your concept release, you portray that omniscient SEC is in possession of omnipotent guidance for all levels of detail, but inclined to dribble particulars out of its secret stockpile only under sustained pressure. You are in grave danger of tripping again on this ruse perpetuated by the regulated. Not only is the SEC guidance library non-existent, you have no reference standards that could recognize one if it were given to you. Remember, once you give your constituents the checklists they seek, your cause is lost. It is to their advantage for you to treat the relationship as a partnership sharing the same goals, while the real scene is code/decode.

External Auditing (II.10, II Pg.11)
The brute fact, in today's transient scene, is that external annual audit practice is often worse than a waste of resources. What is practical and effective auditing in times of stability and equilibrium bears no resemblance to practices effective with frequent and abrupt change. Like the SEC, external audit is constrained to hindsight and crisis response practices. By the time it does its job finding the discrepancies, the money is long gone. Inherent external audit constraints preclude *prevention* of waste, fraud and scandal.

When disturbance to business as usual is the norm, periodic external auditing fails in two ways. It is so far removed from the operational workface; the firm can go bankrupt between audits. In any control intending to keep the system within operating limits, the more turbulent the environment the closer the detection of abnormal must be to the workface. For some upset potentials, the detection must be real time or anticipatory. The low utility function of external auditors has nothing at all to do with their competencies or the analytical repertoire of their discipline. Lag and hierarchical distance determine the zone of the possible. Protection cannot be obtained through any amount of resources that are remote from the workface by hierarchy and time. This is why automatic sprinklers are installed in the same room where a fire might be.

The more dynamic and evolving stakeholder protection becomes, the closer the compliance process must be to the institutional workface. The very idea that an annual invasion by external auditors will safeguard stakeholders for the year to come is ludicrous. Distance is also a fatal flaw of COSO (II.8). The only discipline superglued to the workface arena is internal audit/control. The SEC doesn't even know what the discipline, invented and shaped by management, does.

The size controversy (III.13, 15, 16 & 21, V.35)
The challenge of institutional size is that small companies cannot afford to distrust their staff and survive. As the record shows, large corporations cannot afford to trust anyone. The only level where size merges into common ground is goals. The farther your rules dig down into practices, the more the disparity widens (II.1). Your quest to bifurcate rules of action based on size is doomed to fail.

There is no reason why a large corporation cannot attain stakeholder protection by using accounting and auditing practices that eliminate the need to trust anyone. There is no reason why a small company cannot attain stakeholder protection with individuals ensconced in a working environment that engenders trust.

Because the two issues are coupled, the new SEC rules on disclosure of executive pay, a detailed map for finding a successful bypass, have made the tough internal control/audit task to align with investor protection, hopeless. To reach its goal around the new rules, management will invent more complex and brazen schemes buried in the internal control labyrinth or use an arena outside of internal audit scope. Too bad all the diverse commentary had such little effect.

Fraud controls (III.17)
Whenever the matter of fraud controls is handled as a separate "discipline" needing specialist attention, the cause for preventing fraud is lost. Stakeholders can only be protected from fraud damage by pragmatic foresight at a location close enough to the workface so that fraud appears on the radar screen at its inception - when it will be indistinguishable as fraud from any other error. The record shows treating fraud and

embezzlement apart from internal audit gains very little over what internal audit detects through day-to-day operations.

The SEC is commended for enabling this convenient method for providing commentary.

William L. Livingston, PE