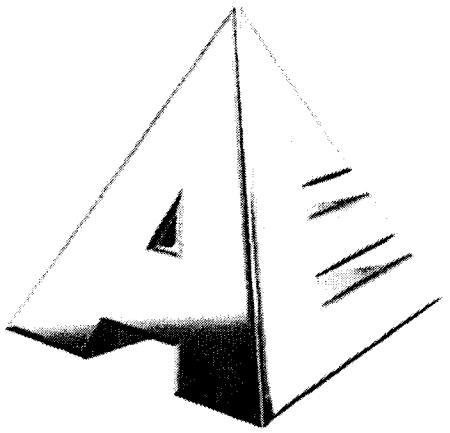


Accelerated Edge™ Incorporated

16541 Redmond Way Suite 417
Redmond, WA 98052
425-829-0717

mmurry@acceleratededge.com

November 18, 2003

Office of the Secretary
PCAOB
1666 K Street NW
Washington, D. C. 20006-2803

Ref: PCAOB Rulemaking Docket Matter Number 008

Dear Mr./Ms. Secretary:

Thank you for the opportunity to comment on the proposed Auditing Standard (the "Standard"). As a director of public and private companies, my interest is in enhancing the quality of information available to exercise my fiduciary duty to protect the interests of shareholders. One source of facts on which directors rely is the external audit.

I commend the PCAOB for including in the definition of internal controls "operating efficiency and effectiveness and compliance with applicable laws and regulations" (page 4) and in the audit standards a review of ". . . controls that focus primarily on effectiveness and efficiency of operations or compliance with laws and regulations. . . ." (Appendix A, Paragraph 14, p. A-11) The definition goes on to incorporate "safeguarding of assets."

These three factors: operating efficiency and effectiveness, compliance with laws and regulations and safeguarding of assets are at the crux of regaining shareholder confidence. Financial statements, after all, represent the results of operations and corporate conduct.

Illegal, illicit or the ***appearance*** of unethical corporate behavior is what shakes shareholder confidence. Section 302 of the Sarbanes-Oxley Act requires executives to certify information contained in reports "fairly present in all material respects the financial condition and results of operations of the issuer." It requires both "financial condition" ***and*** "results of operations." It is a misstatement of material fact for executives to certify they have reviewed their controls and processes and found them to be effective when they turn a blind eye to illegal and unauthorized activity. The legal exposure and subsequent headline risk to the business materially impacts a company's performance.

Legal proceedings are lengthy, costly and disruptive to operations. If a company is at risk for violating a law – whether knowingly or unintentionally – stakeholders require a heads up. Stakeholders relying on the accuracy of

financial statements must have confidence that the reports reflect adherence to all laws and regulations. They expect the audit to confirm (1) companies run well, (2) assets are protected, (3) corporate conduct is responsible and (4) companies obey the law.

With the thought in mind that financial reports ***represent*** the operating condition and corporate conduct, the proposed Standard does not go far enough to protect interests of stakeholders. Throughout the document, the Standards hedge on the real meat of the audit by qualifying ". . . which also have a material affect on reliability of financial reporting." In Appendix C the Standards capitulate on the strength of the protection of assets by citing: "the auditor is not required to understand and test controls over management's decision-making processes for all sales and acquisitions." This hedge enables auditors to overlook processes that affect the company's ability to operate within the law. While it is inappropriate for the auditor to second-guess management's decision-making, it should be on the auditor's radar screen whether processes or lack of controls fail to protect assets, cause the company to run poorly or permit the company to break laws or violate regulations.

Case in point, software license compliance. When management permits employees to load software on company computers without prior authorization and proper documentation, it not only violates agreements with software developers, it is a federal crime. Fines, fees, damages and settlements are material. Yet failure to have internal controls to prevent the illegal activity is a dereliction of management responsibility.

By limiting the audit to those information technology controls on which other controls are dependent (#41 page A-20), instead of focusing on the real meat of shareholder concern and the intent of Congress, auditors are focused on reviewing software code rather than auditing the events, processes and procedures the reports ostensibly represent. Excluding from consideration specific legal requirements all companies are expected to adhere to, the PCAOB gives tacit approval to auditors to ignore adherence to laws. The use of software without proper licenses and proofs of purchase is material, affects operating results and impacts the financial reports which represent those results of operations.

While the Standard requires audit of information technology general controls, its lack of spelling out for auditors the inclusion of acquisition, deployment, implementation, use and disposition of software – whether packaged or custom developed – has enabled audit firms to omit it from their internal control testing in their audit plans.

The emphasis on financial reporting rather than the events and activities the statements represents defies the intent of Congress and fails to protect shareholder interests. It serves merely to mollify and shield auditors from making attestations about company operations, giving them wiggle room when called to task.

The Securities and Exchange Commission recognizes the COSO framework in its adoption of Final Rule: Management Reports on Internal Controls Over Financial Reporting and Certification . . . "The scope of internal control therefore extends to policies, plans, procedures, systems, activities, functions, projects, initiatives and endeavors of all types at all levels of a company." The final rule defines internal control over financial reporting as "a process . . . to provide reasonable assurance regarding the reliability of financial reporting. . . . and includes those policies and procedures that . . . (3) provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the registrant's assets that could have a material effect on the financial statements."

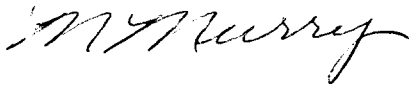
The Standard recognizes operational considerations and incorporates tone-at-the-top and "adherence to laws and regulations" in the control environment. It is simple to test the control environment, tone-at-the-top, the integrity

and values of top management and corporate culture. If management cannot produce one license plus proof of right to use the license (proof of purchase) and chain of ownership (record retention) for each instance of a program found on company computers, the courts have upheld the company is out of compliance. This black-and-white, open-and-shut approach is telling of a management that allows unethical practices to run rampant in a company and has dire consequences on company performance and financial results.

U.S. businesses lose $2.2 billion annually from unlicensed use of software. It is material. A review of the MultexInvestor database on November 14, 2003 reveals that for 16% of all public companies, misuse of software assets would have a material impact on results. For 28% of public companies, the average settlement in litigation involving misappropriation and misuse of software indicates a significant deficiency.

The PCAOB should require auditors to attest to the efficiency and effectiveness of operations, effectiveness of controls and processes designed to protect assets and assure adherence to laws and regulations. I ask the PCAOB to adopt strong audit requirements for effectiveness of processes and controls for adherence to laws and specifically, software license compliance. The alternative is to force government agencies and the courts to impose further regulation on U.S. business. It is far preferable it remain the domain of self-regulatory environment rather than revert to government oversight.

Respectfully submitted,



M. Murry
Chief Executive Officer
Accelerated Edge Incorporated