Sarbanes-Oxley Standards Interpreted by PCAOB

Public Company Accounting Oversight Board

Overview information

The Public Company Accounting Oversight Board (PCAOB) is a private-sector, non-profit corporation, created by the Sarbanes-Oxley Act of 2002, to oversee the auditors of public companies in order to protect the interests of investors and further the public interest in the preparation of informative, fair, and independent audit reports.

On March 9, 2004, the PCAOB issued their official standard for interpreting the Sarbanes-Oxley Act. The official title of that document is: "Auditing Standard No. 2 (AS#2): An Audit of Internal Control over Financial Reporting Performed in Conjunction with an Audit of Financial Statements."

AS#2 compliance for companies considered accelerated filers under the Securities Exchange Act Rule 12b-2 is required for fiscal years ending on or after November 15, 2004. Other companies have until fiscal years ending on or after July 15, 2005, to comply.

Several paragraphs of commentary

After a ten-page introduction, the published PCAOB standard presents 110 pages of detailed requirements (216 of them, to be exact) followed by another 91 pages of auditor report samples, exhibits discussing materiality findings, and responses to public comment on the standards draft. Despite the page volume, the standards are not nearly as detailed as one might expect. When contrasted with the more specific standards issued by COBIT, for example, AS#2 requirements have more room for interpretation.

Interestingly, the limited number of specific examples provided by AS#2 direct auditors' attention to an infinitesimal level of internal control detail. Examples provided include discounts granted by salespersons without proper financial oversight, allocation of R&D costs to divisions, and changes in shipping terms that effect the profit on an order. The rationale is that many otherwise insignificant transactions can be viewed in the aggregate as a material deficiency if the internal controls governing those transactions are not well designed and/or observed.

The net impression is that external auditors have been empowered by AS#2 to go everywhere in the enterprise. If R&D allocations between operating units are suggested as an audit subject, then what would prohibit auditor analysis of concepts like allowances granted for off-quality merchandise, cost of sales variances, future purchase commitments to material suppliers, obsolete material identification and scrap allowance, allocation of manufacturing overhead, advance media commitments, accruals for promotion fulfillment, professional service retainers, sales incentive programs, vacation pay accruals, and on and on?

CFO magazine published an interesting article in their May 2004 issue which provides additional insight; this quotation is from that article:

> "Moreover, because the auditors are required to test anything materially significant to a company's financial statements, they must look for weaknesses in everything from how entries are consolidated and adjusted to what security controls are in place for accessing corporate technology."

Implications for IT management

AS#2 makes only very high level mention of information systems (*the author did not see the word 'computer' even once in the 216 numbered requirements*). Nevertheless, these two pertinent quotations make it clear that PCAOB intends heavy information systems involvement in SOX audits:

- *" ... the auditor should determine whether management has addressed the following elements: ... Including information technology general controls, on which other controls are dependent."*
- *" ... Information technology general controls are part of the control activities component of internal control ... "*

Now, since AS#2 enables (and encourages) auditors to dig into great detail across nearly every business process, and given that those details are processed by and stored within your iSeries, then the implication is that IT management will be in the middle of SOX audit preparations and will be fully engaged when the external auditors arrive for the "real thing."

Recommendations for IT management

It would almost be easier if AS#2 presented a '20 Page Checklist for the IS Manager." Lacking that, Unbeaten Path recommends that "general" information technology controls be firmly established. These are the specific steps that are well advised, in our opinion, based upon: i) the contents of AS#2 (pertinent excerpts presented **here**), and ii) good practice as defined by information processing standards outlined in the 'alphabet' of systems security and data integrity regulations:

a) Acquire a risk assessment from a respected *external* source to identify vulnerabilities in iSeries security procedures and to recommend strategies to mitigate identified risks. The quality of the documentation should be exceptionally high so that external auditors will feel comfortable accepting the results without further testing.

b) Fix the vulnerabilities identified in point a.

c) Re-execute point a after the vulnerabilities have been fixed.

d) Implement a data integrity software that monitors all changes to crucial iSeries data so as to i) establish individual accountability for each change, ii) enable reconstruction of events, and iii) provide the what/when/where/how information needed to identify and correct internal control problems.

e) Adopt a process of archiving old data in a way that permits application software to reacquire access to that information as if it had never been removed from your production files. (Archiving is the antithesis of the insufficient "backup-then-purge" strategy.)

By the way, the 'alphabet' of systems security and data integrity standards includes: COBIT, 21 CFR Part 11, GLBA, HIPPA, UCCnet, NIST 800, ISO 17799, etc. An index to learning more about these IT compliance guidelines/regulations is available **here**.

How Unbeaten Path can help

The following products and services for iSeries hit the PCAOB bulls-eye for SOX compliance:

- **up a notch™ vulnerability assessment and mitigation services**

  Unbeaten Path has helped companies achieve an A+ result on their Sarbanes-Oxley external audit. We address everything from i5 operating system vulnerabilities to software change management, to critical file change observation, to development of world class operational procedures, to compliance issues particular to BPCS / ERP LX software.

- **Bill of Health® Security Diagnostics and R_X for iSeries**

  This product provides 50 robust risk assessment reports describing your iSeries security status together with a competent prescription to address each identified vulnerability.

- **Policy Minder™ Compliance Enforcement software**

  This software has the effect of freezing your i5 operating system security fix once all of the settings have been verified and "blessed" by auditors. Each time the product runs, it identifies any drift between the auditor-sanctioned policies and the current state. Policy Minder provides tools to re-set the operating system configurations to the blessed policy.

- **Stitch-in-Time® Data Integrity Software**

  Quickly and decisively responds to audit challenges about the security of your data. If an unauthorized change was executed in a critical file, **Stitch-in-Time** provides comprehensive information to enable analysis of that change and subsequent risk mitigation.

- **Needle in a Haystack™ Abnormal Event Detection Software**

  Analyzes and self-learns from field-by-field change data accumulated by Stitch-in-Time software. Changes that fall outside the statistical boundaries of that self-learning are immediately reported by e-mail to the pre-designated "guardian" of the pertinent database.

- **Tight as a Drum® Software Change Management**

  Manages the entire software life cycle by controlling everything from registration of a request for change up to an including distribution and unattended implementation of completed work into production environments on iSeries, servers, or clients.

Questions ?

It would be a privilege to answer any questions about these **compliance services and products.** Please contact Milt Habeck. Here's Unbeaten Path International's contact information:

Toll free North America: (888) 874-8008
International: +(262) 681-3151
Send us an e-mail (click **here**)

Unbeaten Path®