

SOX Information

The Sarbanes-Oxley Act



Overview Information

Sarbanes-Oxley Act (SOX) was passed by the United States Congress in 2002 as a response to the creative accounting scandals (e.g. Enron, WorldCom) that caused so much marketplace concern. SOX holds corporate executives accountable for the information reported on key financial statements. SOX also encourages corporations to adopt “separation of duties” policies at the most senior levels of a corporation so as to improve the internal control regime.

Nutshell overview of SOX sections 302 and 404

The two sections of SOX that have the biggest impact on corporations are sections 302 and 404. These sections were designed to improve the reliability and accuracy of corporate financial reporting.

Section 302 requires enterprise management to proactively design and implement steps so as to verify the reliability of internal systems and controls for financial reporting. A corporation must document controls that have a bearing on financial reporting, test them for efficacy, and report on gaps and deficiencies.

Section 404 requires external auditors to provide an annual written opinion about the effectiveness and comprehensiveness of the Section 302 compliance steps that have been implemented by corporate management. This written opinion will be included in the company’s annual report.

Click [here](#) to inspect the actual text of sections 302 and 404.

Formal interpretation of SOX requirements

In March '04 the Public Company Accounting Oversight Board (PCAOB) published the final version of Auditing Standard #2 (AS#2) which interpreted the requirements of SOX for the auditing profession and set compliance deadlines. Click [here](#) to see a three-page summary of the PCAOB standards.

Compliance ideas from Unbeaten Path

Unbeaten Path has several products which hit the bulls-eye on the red-ink recommendations quoted from the magazine article above.

Stitch-in-Time[®] data integrity observation 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. The product works without any changes to your programs or files.



Compliance ideas from Unbeaten Path, *continued...*

Needle in a Haystack[®] detection of System i data mistakes

The product uses artificial intelligence to learn which entries in a database are “normal.” Whenever a data entry falls outside the norm, it immediately sends an email alert to the database guardian, permitting the mistake to be fixed before bad data is propagated. That saves time and money as well as reducing corporate risk and legal exposure.

By Invitation Only[®] user security management for BPCS / ERP LX

Greatly simplifies the definition, maintenance, deletion, and documentation of BPCS/ERP LX user authorization information. It makes it easy for a security administrator to welcome users into only those parts of BPCS that are “right” for them.

By Invitation Only is one of Unbeaten Path’s **Stocking Stuffers**[™] for SOX products invented by experts in BPCS functionality and database design. [Click here](#) for more security software ideas designed specifically for BPCS/ERP LX.

Due Diligence[™] separation of duties auditor for BPCS / ERP LX

Identifies and reports separation of duties conflicts based on internal control principles and best business practices. The product’s search design is in harmony with regulatory requirements authored by Sarbanes-Oxley and the rest of the compliance alphabet: PCAOB, 21 CFR part 11, GLBA, COBIT, etc.

Bill of Health[®] security diagnostics and R_x for iSeries

Provides 50 robust risk assessment reports describing your iSeries security status together with a competent prescription to address each identified vulnerability. The quality and third-party objectivity of these reports will impress external auditors.

up a notch[™] vulnerability assessment and mitigation

Unbeaten Path consultants have prepared companies well for the degree of scrutiny likely during an external SOX audit. We perform a very thorough assessment and then suggest practical steps to close any observed vulnerabilities. [Click here](#) to see a sample assessment deliverable.

As much detail as you can handle about Sarbanes-Oxley

The Sarbanes-Oxley Act is numbered H.R. 3763; it was passed in the 107th Congress on January 23, 2002. For those of you interested in immersing yourself in some detailed reading material and don’t mind a 66 page .pdf download wait, here you go ...

The full text of H.R. 3763 (see page 33 for Section 302 and page 45 for Section 404)

Opinion and commentary about SOX implications

This **magazine article**: 'Security Patrol: Is the Sarbanes-Oxley Act Security-Relevant or Not?' provides a balanced overview. As you read the article, note that we've used red ink to highlight two SOX security recommendations. Those two suggestions have been extracted from the article and quoted below:

- ◆ Journal the critical data files to capture details of each change made to the file.
- ◆ Implement the concept of "least privilege." That is, give users access only to data and applications that they have a direct need for.

This **opinionated essay**: 'What shareholders should know about the exploding responsibility for data integrity' was composed in the Spring of 2004 by Unbeaten Path's founder, Milt Habeck. Although a few facets of the essay (e.g. UCCnet and the rush for RFID compliance) have grown obsolete, it's surprising how much of the content is still pertinent half a decade later.

Here's a website that provides links to a large number of pertinent news articles as well as some viewpoints and related information from multiple professional accounting groups.

[Public Company Accounting Oversight Information](#)

Other IT compliance standards

Sarbanes-Oxley wasn't the beginning and is not the end of internal control and security regulations pertinent to computer systems. [Click here](#) to navigate to an index of the alphabet soup list of other IT compliance standards.

Questions ?

It would be a privilege to answer any questions about the implications of Sarbanes-Oxley for your company. 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®

