

New SOX Guidance Can Help Cut Audit Costs

French Caldwell

Recent guidance on the Sarbanes-Oxley Act offers the opportunity to scale down the size and expense of internal-controls audits. A new audit standard also encourages controls automation.

NEWS ANALYSIS

Event

On 23 May 2007, the U.S. Securities and Exchange Commission (SEC) issued new interpretive guidance for the Sarbanes-Oxley Act (SOX) aimed mostly at reducing the Section 404 audit costs, and addressing concerns about the impact on small companies, which must comply this year.

On 24 May 2007, the Public Company Accounting Oversight Board (PCAOB) approved a new audit standard, AS-5, which aligns with the SEC guidance and reduces the number of internal controls that external auditors must review (see www.pcaobus.org/Rules/Docket_021/2007-05-24_Release_No_2007-005.pdf). AS-5 is undergoing a 30-day public comment period before final approval by the SEC.

Analysis

The current PCAOB audit standard for SOX, AS-2, settles the power struggle between external auditors and company management squarely on the side of the auditors. Though both the SEC and PCAOB have said that auditors and management should take a top-down, risk-based approach to SOX Section 404 audits, AS-2 and SEC guidance did not facilitate that approach. Rather, following the audit standard, auditors relied very little on work performed by others, and instead reviewed and tested large numbers of internal controls. The costs have been tremendous. An annual survey by Financial Executives International shows year-on-year reductions in 404 internal and consulting costs since 2004, but audit costs have not budged.

The new SEC interpretive guidance clarifies that management, not the auditor, is responsible for an annual review of internal controls, and that the auditor is not required to report on management's evaluation process. The PCAOB's new audit standard, AS-5, focuses the audit on entity-level and IT general controls. It directs the auditor to focus on areas of higher risk, such as the financial close process and management's anti-fraud efforts. There is a strong emphasis on controls automation for applications relevant to financial reporting, with the explicit statement that "an automated control would generally be expected to be lower risk if relevant information technology general controls are effective," and an appendix on "Benchmarking of Automated Controls." AS-5 also provides examples of how to interpret the standard, and specific directions on auditing smaller companies. The directions will be amplified with additional guidance later this year.

RECOMMENDATIONS

Enterprises:

- Engage your auditors now to determine how they will reduce the audit scope and costs. Also, get agreement on a baseline audit of automated controls — and start with a risk-based re-examination of what applications are within scope.
- Focus compliance technology investment on application controls automation first, and, secondarily, on automation of application access controls. Also, determine whether automation can improve the reliability of IT general controls. Beyond these three areas, compliance technology business cases should require significant additional (that is, non-SOX) process improvement benefits and demonstrable return on investment.

- If financial process improvement and application replacement are under consideration, consider advancing the timeline. Simplification and rationalization of financial processes for business performance reasons will also yield compliance benefits: If processes and applications are the same across multiple business units, controls can be standardized, simplifying compliance management, and auditors can test controls just once, in one location.

IT organizations:

- Focus on IT general controls and on improvements in IT governance. Good governance and good general controls should indicate to auditors that underlying, more-granular controls do not need detailed reporting and audits.

RECOMMENDED READING

- "The 2007 Compliance and Risk Management Planning Guidance: Governance Becomes Central" — Focusing on better governance is the only way to reconcile the objectives set by regulatory requirements and the demands for improved organizational performance. **By French Caldwell**
- "Use Best Practices to Negotiate Sarbanes-Oxley Compliance With Auditors" — Agreements negotiated with your auditor should balance meeting the letter and intent of SOX with doing what's appropriate for your organization. **By Christine Adams and Paul Proctor**

(You may need to sign in or be a Gartner client to access the documents referenced in this First Take.)

REGIONAL HEADQUARTERS

Corporate Headquarters

56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters

Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters

Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters

Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters

Gartner do Brazil
Av. das Nações Unidas, 12551
9º andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509