

## **The Sarbanes-Oxley Act: Time is *not* on your side**

**October 2004**

Understanding and insuring compliance with the Sarbanes-Oxley Act of 2002 (SOX) can be an enormous undertaking. SOX, almost to understate things, is “complex legislation,” and compliance with it demands a serious and well-planned and executed approach. This article will present an overview of SOX and discuss some of the consequences and requirements of SOX compliance.

### **Expert Insight**

According to AMR Research, 85 percent of companies predict that SOX will require them to make at least *some* changes to their IT and applications infrastructure. John Hagerty, vice president of research at AMR, says SOX projects will be given high priority. In his view, many executives view SOX compliance as an opportunity to make overdue IT investments. “Vice presidents of IT and CIO’s are telling us they are using



Information Alternatives • 9850 Redhill Drive • Cincinnati Ohio 45242 • 513.793.2929 • www.infoalt.com

SOX as the justification for broad-based process and/or technology improvement projects,” Hagerty says.<sup>1</sup>

Perhaps another way to view SOX compliance, then, is as a way to “tighten the IT ship.”

### **Sarbanes-Oxley: What it is**<sup>2</sup>

The U.S. Public Company Accounting Reform and Investor Protection Act of 2002, typically known as the Sarbanes-Oxley Act (SOX), is the single most dramatic regulatory reform of publicly traded markets since the Securities and Exchange Act of 1934. SOX was designed to sharply reduce corporate malfeasance and conflicts of interests, while improving transparency and bolstering public confidence in the stock markets. SOX was born in response to the sensational corporate scandal cases of Enron and other large publicly traded companies. As with all new sweeping regulatory changes (and this one is fluid and involves criminal penalties for non-compliance) SOX has created an environment of fear, uncertainty and doubt, and many companies lack clear direction on how to proceed – but not when to proceed, because for many companies the deadline is December 31, 2004.

Although SOX does not directly regulate companies’ information technology infrastructure, IT is the foundation of and pathway for the financial data and information processes and controls that the law describes and requires. Therefore, a company’s IT department will play a central role in achieving compliance.

Few sections of the lengthy SOX rules directly affect a company’s IT department; however, it is important for IT executives and managers to understand the salient rules to most efficiently become compliant. The key compliance rules of SOX are contained in sections 302 and 404. Moreover, the Gartner Group expects that section 409 will affect IT projects within one year after 404 filing deadlines pass in 2004.<sup>3</sup>

### **Certification of Financial Reports (section 302)**

According to section 302, the CEO, CFO and an attesting CPA firm must certify the accuracy of financial statements and accompanying disclosures in the financial reports, and that those statements fairly present “in all material aspects the operations and financial condition of the issuer.” Section 302 further prescribes criminal penalties if CEO’s or CFO’s knowingly issue false or misleading statements. Additionally, section 302 requires material facts that are used to generate financial reports be retained and made available to the public. In most companies, application software systems generate the financial reports and manage *e-mail* systems and traffic. For most companies, *e-mail*

---

<sup>1</sup> CIO.com

<sup>2</sup> Sarbanes-oxley-forum.com

<sup>3</sup> Gartner.com



Information Alternatives • 9850 Redhill Drive • Cincinnati Ohio 45242 • 513.793.2929 • www.infoalt.com

has become the primary tool for distributing this information internally. IT departments are being asked to certify that these systems are secure and reliable. Because of the criminal penalties, CIO's (and/or CTO's) also should expect to be asked to sign an internal attestation on their systems to further protect the enterprise in case of CIO/CTO negligence in maintaining these systems.

### **Certification of Internal Controls (section 404)**

Section 404 is the primary driver of SOX compliance efforts and is the most significant section for corporate IT departments. This section requires certification of management's responsibility for establishing and maintaining adequate internal control over financial reporting for the company, attested to by the company's auditor, and personally attested to by the CEO and CFO. This certification includes an assessment of the controls and identification of the parameters used for the assessment. While section 302 requires that financial statements be accurate and complete; section 404 requires that the **processes** that are used to create statements be accurate and meet an accepted standard.

Since the processes and internal controls are implemented primarily in application software systems, section 404 audits must involve a detailed assessment of these systems. Moreover, process changes undertaken to achieve compliance – generally called remediation – must be built, documented and implemented by the company's IT department or outside remediation resources. It is possible that a completely paper-based organization could be compliant; however, most organizations make such extensive use of technology for financial reporting that IT must play a major role in both auditing and remediation projects. Section 404 also requires the reporting of "material process changes" each quarter. This means that a new Supply Chain Management (SCM) system or material change to an existing application system may require a new 404 audit, remediation and attestation report.

### **Material Event Reporting (section 409)<sup>4</sup>**

Publicly traded companies must disclose information regarding material changes in their financial condition on a rapid and current basis. The goal of section 409 is to protect investors from a delay in reporting of material events, and the risk of increasing their losses. Application software systems – especially financial management and reporting systems, because they support and facilitate operations and financial management – play an important role in the detection and management of material events. Here is where the pre-emptive use of application software systems can enable early detection (and remediation if required) of material events or compliance issues. Suffice it to say that section 409 should be considered as a "work in progress" by the SEC. For example, the SEC has not defined the term "real time" from a process perspective yet. Some sections

---

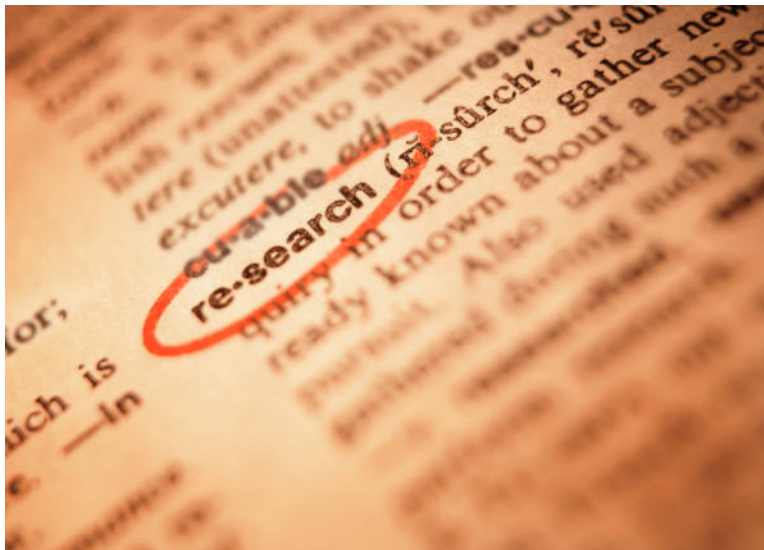
<sup>4</sup> *ibid*



of SOX, although carrying serious consequences for non-compliance are subject to interpretation. We expect this situation to stabilize – eventually.

### **Compliance and the Role of IT**

Public companies must meet section 302 requirements. Moreover, depending on their filing date and size, they must meet section 404 requirements by June 15, 2004 or December 31, 2004 (for large companies, “accelerated filers”) and April 15, 2005 (for smaller companies, including foreign companies who were listed in the United States in 2004.) Many enterprises have just started planning or have already started their compliance projects. Although auditing, remediation and compliance can seem overwhelming and complex, it is from a high level a straightforward process. What follows is a summary of the typical steps involved in SOX compliance.



### **Step 1: Audit**

Publicly traded companies must comply with sections 302 and 404 audits before filing. Therefore, the first step in SOX compliance is to conduct audits to discover where changes need to be made.<sup>5</sup> It should be noted that a provision of SOX is that it restricts the services that the firm performing the audit can provide to prevent conflicts of interests. This means, the auditor cannot offer remediation services to the company just

<sup>5</sup> [sox.weblog.gartner.com/weblog/index.php?blogid=11](http://sox.weblog.gartner.com/weblog/index.php?blogid=11)



Information Alternatives • 9850 Redhill Drive • Cincinnati Ohio 45242 • 513.793.2929 • www.infoalt.com

audited. These audits can be intensive and will require the documentation of the company's financial process and all internal process controls. IT management should expect to participate extensively in the audit, often as a member of a compliance group. Most auditing firms use technology that must be installed in the enterprise's IT systems to document the findings, and to report to management. Such technology should be included in the audit engagement's fees.

## **Step 2: Gap Analysis**

After the initial audit, most companies will need to make at least some process changes that must be reflected in their IT systems. Some changes may be as simple as adding a sign-off in a financial reporting system or as comprehensive as the complete "buttoning up" of an SCM system. IT management should expect that virtually all required changes will be to support non-IT operations requirements, for example, a payroll or accounts receivable process, managed by IT systems. Gartner has concluded that more than 80 percent of remediation will be updates to systems and will *not* require new technology.<sup>6</sup> When new IT is required, it most likely will be a documentation management tool to document controls and manage data that are used to create reports. Your SOX auditor should provide the requirements you need to attain compliance.

---

<sup>6</sup> *ibid*



### **Step 3: Compliance (and remediation)**

Using the gap analysis the next step is remediation – *i.e.*, remedying the affected IT systems. Many companies lack the necessary internal resources for remediation and hire external consultants to assist them. Another reason that companies utilize external resources for remediation is that SOX compliance is a “hard deadline” that can have serious (criminal) penalties. Because of this, project timelines are more important than many companies may be accustomed to; and it is imperative to leave enough time for a follow up audit and “attestation” (and perhaps even further remediation) by the SOX auditor. Again, remember that the attesting SOX auditor cannot provide remediation services, but will need to perform periodic audits (quarterly) to ensure that your company is on track. It is probable that the cycle of audit, remediation/compliance and attestation will be repeated in your organization – regularly.



Information Alternatives • 9850 Redhill Drive • Cincinnati Ohio 45242 • 513.793.2929 • www.infoalt.com

#### **Step 4: File and Get Ready for the Future (*i.e.*, rinse lather, repeat)**

Once your company is in compliance and has issued its periodic report, it's time to get ready for the future. SOX compliance has often been described as "a permanent Y2K"<sup>7</sup> project. Here is why: changes will be made to the SOX regulations, SOX compliance requires audits, remediation and attestations with virtually every periodic report, and disclosures of material events "in real time." IT projects that may affect your financial process must be reviewed and reported quarterly. Thus, a new SCM or other (application software, *e.g.*) IT project or financial upgrade will require new SOX certification. In the near term, IT departments should document *all* changes to systems that may or do change the financial process or internal financial controls, and report these changes, appropriately as to form, to the CEO, CFO (possibly the CIO or CTO) and/or SOX compliance committee, if there is one. In the long term, IT management must develop compliance management procedures and processes to account for SOX compliance needs, with a particular emphasis on records and business process management.

**Conclusion:** Although SOX is a sweeping regulation that creates significant requirements for companies' IT organizations, becoming compliant can be a relatively routine matter. Corporate IT executives – CIO's and CTO's – should work with SOX auditors to understand where their systems are non-compliant and undertake remediation. Because this is a recurring requirement, it should become a line item in your annual IT budget.

*Information Alternatives has been helping companies manage and leverage their technology investments for nearly 20 years. We can help you manage the entire technology lifecycle, from implementation to support to augmentation, including Sarbanes-Oxley Audit & Remediation Services*

*Please contact Chris Willman, Vice president of Business Development for more information.*

*Mr. Willman can be reached at 513.793.2929 x 208*

---

<sup>7</sup> sarbanes-oxley-forum.com