CIO Alert: How You Should Prepare for Sarbanes-Oxley

Sarbanes-Oxley is the most sweeping legislation to affect publicly traded companies since the reforms during the Great Depression. CIOs should follow Gartner’s four-phase approach to meet compliance requirements.

Sarbanes-Oxley is the most sweeping legislation to affect publicly traded companies since the reforms during the Great Depression. CIOs should follow Gartner’s four-phase approach to meet compliance requirements.

IT Is the Backbone of the Processes Regulated by the Law

The U.S. Public Company Accounting Reform and Investor Protection Act of 2002, known as the Sarbanes-Oxley Act, is the most sweeping regulatory reform of publicly traded markets since the Securities and Exchange Act of 1934. Sarbanes-Oxley is designed to reduce fraud and conflicts of interests, while increasing financial transparency and public confidence in the markets. It is a response to the sensational corporate fraud cases of Enron and WorldCom. As with all new dramatic regulatory changes — especially those where rules are evolving and criminal penalties are possible — Sarbanes-Oxley has created fear and uncertainty, and enterprises lack clear road maps.

Although Sarbanes-Oxley doesn’t directly regulate information technology, IT is the backbone of the financial processes that the law regulates. Therefore, the CIO will play a critical role in achieving compliance.

A Sarbanes-Oxley Primer for CIOs

Few sections of Sarbanes-Oxley directly affect the CIO, but it’s important for CIOs to understand the requirements to most efficiently become compliant. Section 302 and section 404 are the primary drivers of compliance projects. Gartner expects that section 409 will affect IT projects within 12 months after 404 filing deadlines pass in 2004.

Section 302: Certification of Financial Reports

The CEO, CFO and an attesting public accounting firm must certify the accuracy of financial statements and disclosures in the periodic report, and must certify that the statements fairly present in all material aspects the operations and financial condition of the issuer. Section 302 prescribes criminal penalties if CEOs or CFOs knowingly or willfully issue inaccurate statements. Section 302
also requires that the material information that is used to generate periodic reports be retained and made available to the public.

In most enterprises, IT systems generate periodic reports and control e-mail, the primary tool for communicating the information internally. CIOs should ensure that those systems are secure and reliable. Because of the criminal penalties, CIOs should expect being asked to sign an internal attestation on their systems to further protect the enterprise in case of CIO negligence in maintaining these systems.

**Section 404: Certification of Internal Controls**

Section 404 is the largest driver of Sarbanes-Oxley compliance projects and the most significant section for IS organizations. It requires a statement of management’s responsibility for establishing and maintaining adequate internal control over financial reporting for the company, attested to by the company’s auditor. This statement includes an assessment of the controls and identification of the framework used for the assessment. Section 302 requires that financial statements be complete and accurate. Section 404 requires that the process used to generate statements be accurate and meet an accepted industry standard — the Committee of Sponsoring Organizations of the Treadway Commission standard is the de facto standard.

Because the processes and internal controls are implemented principally in IT systems, section 404 audits involve a detailed assessment of those systems. Process changes to meet compliance must be documented and implemented by the IS organization. Although a completely paper-based organization could be compliant, most organizations make such extensive use of technology for financial reporting that the CIO plays a major role in auditing and compliance projects. Section 404 also requires reporting of material process changes every quarter. Thus, a new enterprise resource planning (ERP) system or any material change to a system could require a new 404 audit, attestation and report.

**Section 409: Material Event Reporting**

Public companies must disclose information on material changes in their financial condition or operations on a rapid and current basis. The goal of section 409 is to protect investors from delayed reporting of material events, increasing their losses. IT systems, as they support business operations and financial management, play a significant role in the detection and management of material events. Proactive use of IT enables earlier detection and mitigation of material events. The U.S. Securities and Exchange Commission (SEC) hasn’t issued final guidelines for section 409, but Gartner expects that IT systems will be affected by this section in 2004.

The SEC has not defined “real time” from an enterprise information process perspective. Unless the SEC clarifies the time frame, the working guideline for section 409 is disclosure of changes, in addition to the report for that period.

**Compliance Process and Role of the CIO**

Public companies must meet section 302 requirements. Depending on their filing date, they must meet section 404 requirements by 15 June 2004 for large companies and 15 April 2005 for other filers, including foreign companies listed in the United States in 2004. Many enterprises are planning
or have started their compliance projects. Although it seems daunting and complex, from a high level, the process is straightforward.

**Phase 1: Discovery/Audit**

Enterprises must pass section 302 and section 404 audits before filing. Therefore, the first step in compliance is to begin audits to discover where changes need to be made. Gartner advises against “pre-attestation” projects to prepare for the audit by auditors or consultants other than the attesting auditor — they are a waste of resources (see “Don’t Put the Cart Before the Horse,” http://sox.weblog.gartner.com/weblog/index.php?blogid=11). A good provision of Sarbanes-Oxley is that it limits the services that an attesting audit firm can offer to prevent conflicts of interests. Thus, the auditor that signs your financial statement can’t implement recommended changes through some future project.

These audits are fairly intensive and involve the documentation of the enterprise’s financial process and all internal process controls. CIOs should expect to participate extensively in the audit process, usually as a member of a compliance committee. You may have to dedicate resources to support the examination of IT systems and financial data. Most auditing firms use technology that must be installed in the enterprise to document the process and results, and to communicate with management. That technology will be included as part of the project — you should never pay for it.

**Phase 2: Gap Analysis**

After the first pass of the audit, most enterprises will have to make a variety of process changes that must be reflected in technology. The change may be as simple as adding a sign-off in a financial package or as complex as the complete retooling of an ERP system. CIOs should expect that most required changes will be to support non-IT process requirements, such as an accounts payable process, managed in IT systems. Gartner anticipates that more than 80 percent of changes will be updates to systems and will not require new technology. When new technology is required, it will likely be a documentation and records management tool to document controls and manage records that are used to generate reports. Your attesting auditor should provide a complete list of requirements to meet compliance.

**Phase 3: Compliance**

With the gap analysis from your auditor in hand, implement required changes in IT systems. If you lack internal resources, consider hiring external consultants to assist you, but bound them by the requirements from your auditor to prevent “scope creep.” Understand that Sarbanes-Oxley compliance is a hard deadline with serious penalties. Thus, project timelines are more important than you may be used to, and you must leave enough time for a final audit and attestation by your auditor. Also remember that your attesting auditor can’t implement the required changes, but it can perform periodic evaluations to ensure that you are on track and should participate in any compliance project.

**Phase 4: File and Prepare for the Future**

Once your final audit and attestation are complete and your company has issued its periodic report, it’s time to prepare for the future. Sarbanes-Oxley has been described as “Y2K without an end date.” Not only will changes be made to the regulation, but it requires audits and attestations with every
periodic report, and disclosures of material events as they occur. IT projects that might materially affect your financial process must be evaluated and reported quarterly. Thus, a new ERP project or financial upgrade will require new certification. In the short term, CIOs should document changes to systems that potentially change the financial process or internal controls, and report these changes to the CFO, CEO and risk management or compliance committee, if one exists. In the long term, CIOs should develop compliance management architectures (see “Compliance Management Reduces Regulatory Burdens,”) to account for long-term compliance needs, with a particular emphasis on business process management and records management.

**Don’t Buy New Software This Year**

As with any change to how you conduct business, various solutions have emerged to take advantage of potential new market opportunities. However, now is not the time to invest in new IT projects related to compliance. Gartner continually evaluates old and new software solutions and services, but we have not seen any “must have” Sarbanes-Oxley solutions. No technology panacea is available — working with your auditor and implementing changes is the only way to become compliant. CIOs should focus resources on meeting the compliance needs discussed above. Beware of software solutions that “solve” Sarbanes-Oxley or propose dramatic cost reductions to meet compliance. Investing in such solutions diverts financial resources before you know your exact needs and, with filing deadlines approaching, it can divert necessary internal resources.

Some technologies will play an important role in meeting compliance and improving business performance in the term. Gartner offers a timeline for when you should invest in various technologies on your path to implementing a long-term compliance architecture (see Figure 11).

---

**Figure 11**

**Timeline for Sarbanes-Oxley Compliance**

<table>
<thead>
<tr>
<th>March 2004</th>
<th>1Q05</th>
<th>Year-end 2005</th>
<th>2006</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complete updates to IT systems as required by auditors</td>
<td>Evaluate a business process management solution</td>
<td>Implement business process management</td>
<td>Evaluate and implement a risk management dashboard. Link with BPM and financial/ERP systems</td>
</tr>
</tbody>
</table>

Source: Gartner

BPM = business process management  
ERP = enterprise resource planning

---

**Tactical Guidelines**

- Understand your responsibilities to meet compliance by working with the corporate auditor to find process and internal control flaws in IT systems.
• Champion the expenditure of resources to meet compliance goals on the shortest realistic timeline.

• Implement required changes; use external assistance if you lack internal resources.

• Prepare for future compliance needs once your first successful attestation and filing is complete.

**Strategic Planning Assumptions**

• Through 4Q04, public corporations will spend less than 20 percent of their Sarbanes-Oxley budget on new IT (0.8 probability).

• By 2005, 70 percent of publicly traded companies will require CIOs to sign attestations on the reliability of financial IT systems, as well as CIO compliance with Sarbanes-Oxley and other regulations (0.7 probability).

**Bottom Line**

• Although Sarbanes-Oxley is a sweeping regulation with significant impact on IT, becoming compliant is straightforward.

• CIOs should work with their auditors to understand where their systems are noncompliant, then implement required changes.

• Brace yourself for possible unplanned expenses.

Written by Edward Younker, Research Products

Analytical source: Rich Mogull, Debra Logan and Lane Leskela, Gartner Research

For related Inside Gartner articles, see:

• “Sarbanes-Oxley Financial Rules Will Challenge IS Organizations,” (IGG-06252003-05)

• “Management Alert: The Sarbanes-Oxley Act Will Affect Your Enterprise,” (IGG-04022003-02)