Sarbanes-Oxley Compliance:
Section 404-Past, Present, and Future

BADM 590/395 IT Governance MS1

Professor Michael Shaw

Submitted by: Amy Smith

BA in MIS

University of Illinois at Urbana-Champaign
Abstract:
As internal control monitoring and reporting becomes routine, companies will need to adopt a more comprehensive solution and develop long-term strategies to ensure Section 404 compliance. In my paper I will begin by giving an overview of the Sarbanes-Oxley Act, focusing on Sarbanes-Oxley compliance, specifically Section 404. I will discuss impediments to the process of developing a long-term strategy, as well as proposed solutions, mainly implementing business process management software. I will cover the short-comings of current documentation warehouses as well as the advantages of employing business process management software. Ultimately, I hope to emphasize the need for companies to develop and implement a long-term strategy to ensure Section 404 compliance.

Sarbanes-Oxley Act: Overview
The Sarbanes-Oxley Act was named after sponsors Senator Paul Sarbanes and Representative Michael G. Oxley. The Sarbanes-Oxley Act of 2002, also called the Public Company Accounting Reform and Investor Protection Act of 2002 and commonly called SOX or Sarbox, is a divisive United States federal law passed in response to a number of major corporate and accounting scandals and represents the biggest change to federal securities laws in a long time. Some of the major companies involved in these scandals were Enron, Tyco International, Peregrine Systems and WorldCom (recently MCI and now currently part of Verizon Business). These scandals resulted in substantial decrease of public trust in accounting and reporting practices. The legislation is wide ranging and establishes new or enhanced standards for all U.S. public company boards, management, and public accounting firms. Sarbanes-Oxley is not a set of business practices and does not specify how a business should store records; rather, it defines
which records are to be stored and for how long. The legislation not only affects the financial side of corporations, but also the IT department, whose job it is to store a corporation's electronic records. The Act contains 11 titles, or sections, ranging from additional Corporate Board responsibilities to criminal penalties, and requires the Securities and Exchange Commission (SEC) to implement rulings on requirements to comply with the new law. As far as compliance is concerned, the most important sections within these are often considered to be 302, 401, 404, 409, 802 and 906. Supporters of these reforms believe the legislation was necessary and useful; but critics argue that it does more economic damage than it prevents. However, those who have studied the law point out how modest the Act is in comparison to the heavy rhetoric accompanying its passage and adoption.
The Sarbanes-Oxley Act's major provisions include the following:

- Creation of the Public Company Accounting Oversight Board (PCAOB)
- A requirement that public companies evaluate and disclose the effectiveness of their internal controls as they relate to financial reporting, and that independent auditors for such companies "attest" (i.e., agree, or qualify) to such disclosure
- Certification of financial reports by chief executive officers and chief financial officers
- Auditor independence, including outright bans on certain types of work for audit clients and pre-certification by the company's Audit Committee of all other non-audit work
- A requirement that companies listed on stock exchanges have fully independent audit committees that oversee the relationship between the company and its auditor
- Ban on most personal loans to any executive officer or director
- Accelerated reporting of insider trading
- Prohibition on insider trades during pension fund blackout periods
- Additional disclosure
- Enhanced criminal and civil penalties for violations of securities law
- Significantly longer maximum jail sentences and larger fines for corporate executives who knowingly and willfully misstate financial statements, although maximum sentences are largely irrelevant because judges generally follow the Federal Sentencing Guidelines in setting actual sentences
- Employee protections allowing those corporate fraud whistleblowers who file complaints with OSHA within 90 days to win reinstatement, back pay and benefits, compensatory damages, abatement orders, and reasonable attorney fees and costs.

(wikipedia.org/sarbanes-oxley act)
Section 404: Management Assessment of Internal Controls

Section 404 is historically the most argued of the Sarbanes Oxley Act sections as companies strive to meet compliance. All annual financial reports must include an Internal Control Report stating that management is responsible for an "adequate" internal control structure, and an assessment by management of the effectiveness of the control structure. If there are any shortcomings in these controls, they must also be reported. In addition, registered external auditors must attest to, or bear evidence of, the accuracy of the company management’s contention that internal accounting controls are in place, operational and effective.

A direct excerpt from the Sarbanes-Oxley Act of 2002 report for section 404:

(a) Rules Required. The Commission shall prescribe rules requiring each annual report required by section 13(a) or 15(d) of the Securities Exchange Act of 1934 to contain an internal control report, which shall:

(1) state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and

(2) contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.

(b) Internal Control Evaluation and Reporting. With respect to the internal control assessment required by subsection (a), each registered public accounting firm that prepares or issues the audit report for the issuer shall attest to, and report on, the assessment made by the management of the issuer. An attestation made under this subsection shall be made in accordance
with standards for attestation engagements issued or adopted by the Board. Any such attestation shall not be the subject of a separate engagement. (http://www.sarbanes-oxley-101.com/SOX-404.htm)

The PCAOB suggests considering the Committee of Sponsoring Organizations of the Treadway Commission (COSO) framework in management/auditor assessment of controls. Auditors have also looked to the IT Governance Institute's "COBIT: Control Objectives of Information and Related Technology" for more suitable standards of measure. This framework focuses on information technology processes while keeping in mind the big picture of COSO's "control activities" and "information and communication". However, there are certain aspects of COBIT that are outside the boundaries of Sarbanes-Oxley regulation.
SOX 404 Compliance: Past

Most organizations have implemented paper and MS Excel-based processes to document and test internal controls over financial reporting to comply with Section 404 of the Sarbanes-Oxley Act. These organizations spend a large amount of time and effort in:

- scheduling tests
- manually testing the internal controls
- identifying and tracking remediation
- compiling and cataloging evidence
- implementing change control
- managing the entire process.

Companies are coming to the realization that such an approach is markedly resource intensive and significantly increases the cost of compliance. In addition, it increases the risk of non-compliance, where penalties can be severe. They include prison, fines, firings, accounting overhauls, public censure, stock devaluation and bankruptcy. By following the steps mentioned below companies can lower their SOX 404 compliance costs, reduce their non-compliance risk and free up their personnel to focus on activities that deliver real benefit to the bottom line.

- integrating the design and testing of internal controls over financial and IT processes
- providing a risk-based approach to rationalizing controls
- automating the testing of certain financial and IT controls
- providing a mechanism to increase visibility and control over the entire compliance process
Limits of a Documentation Warehouse:

Because of Sarbanes-Oxley, companies are now required to maintain documentation of significant business processes and their related controls. As business processes change, two things must happen:

- The existing controls related to the previous business process must be evaluated and, if necessary, changed to reflect the new process, and
- The company’s documentation must be updated to reflect the changes to both the process and the control

The problem with a data warehouse solution is that these two tasks are not automated, which requires manual intervention. Over the long term, the inability to accommodate evolutions in the company’s business process will increase the costs of SOX 404 compliance.

Changes to business processes require the reevaluation and possible change to the control procedures that ensure processing accuracy. As business processes change, the necessary changes to internal control insulate, not being implemented until after processing errors occur.

The second problem that may occur is that the company makes changes to its processes but fails to simultaneously update its warehouse of process and control descriptions. Under the Sarbanes-Oxley rules, documentation that does not reflect the company’s current procedures is also a control deficiency that the company may have to report to its shareholders.

In effect, the limits of a data warehouse solution create an extra level of required controls to ensure that controls are reevaluated and modified when business processes change and that the
documentation database is updated accurately and on a timely basis when changes do occur. It is an unnecessary and cost-ineffective level.

A spreadsheet solution, which many companies have adopted in the first year of implementing SOX 404, does not solve the problems inherent in a compliance tracking solution. In fact, because of their lack of report writing capabilities and relative inability to pre-define the form and content of input, spreadsheets may create more problems in the long run than they solve in the short run. Invariably, the quality of the information will vary greatly, depending on who did the input, and management will grow wary of scrolling through endless columns of detail to find the information they need to assess control effectiveness. The whole process is very inefficient.

**Sarbanes-Oxley Section 404: Looking Ahead**

Business process management software automates the process of evaluating old controls and updating outdated documentation.
Benefits of automating the SOX process:

**Reduced Compliance Costs:**

By automating the SOX processes, companies significantly reduce the time being spent by internal staff and/or consultants on SOX related activities. Employees will be able to carry out team activities in a much more productive manner with the collaborative environment that automation provides. Typical expected savings through automation of SOX processes can range from 25-40%.
**Improved Control on the Process:**

Automation can enforce a consistent process across the enterprise, eliminating any deviations and error that cost the company in terms of additional cost and time associated with repeated processes and multiple checks that need to be performed.

**Better Resource Utilization:**

With the entire SOX process streamlined and automated, companies can better utilize its resources by moving many tasks down the responsibility chain. Process owners can take direct responsibility for managing internal controls, and auditors can focus on testing key controls and project oversight. The dependence (and costs) on external auditors will also be significantly reduced.

**Lower Exposure:**

Executive dashboards provide enterprise-wide visibility into the compliance process and highlight issues that need to be addressed immediately. The solution has the ability to track design status, process ownership, assessment plans, etc. on graphical charts that can be accessed globally and display real-time information. The complete visibility provided by automation lowers the risk of non-compliance and associated penalties. Executives can be assured of higher customer and investor confidence.

**Streamlined Change Control:**

Integrated document management provides access control and change control capabilities. Access control ensures only the right people can access or change the data/documents. Change controls keep documentation and processes in sync and significantly reduce the amount of redo of documentation in following years.
Moving toward a SOX 404 Business Management Solution

“To be suitable for Sarbanes-Oxley compliance, business process management tools must, at a minimum, be capable of the following.

• Capture Necessary Information: The detailed rules implementing the Sarbanes-Oxley requirements describe specific requirements for the contents of a company’s documentation of its processes and controls. Any software solution management adopts for Sarbanes-Oxley must be able to capture these required elements efficiently.

• Reporting Flexibility: Ultimately, a company must evaluate the effectiveness of its internal control system as a whole. To make that kind of overall assessment requires management to look at different groupings of individual controls. For example, it may need to look at all controls related to the sales/accounts receivable cycle or all those affected by its order entry system. The best software solutions currently available have robust report writing capabilities, which must be matched if business process management software is to be effective.

• Audit Trails: To take full advantage of all the benefits that a business process solution provides, the software must be able to generate a variety of audit trails. The system must capture and promptly report to management all changes to business processes and controls. It also must track the processing of all transactions and identify all instances where established procedures were not performed timely for subsequent follow up.

• Security: Sarbanes-Oxley requires companies to appoint an external auditor to audit its controls.
This audit requirement elevates the importance of the company’s processes and controls, and the related documentation becomes vital information whose integrity must be protected. Logical access control features should be built in to the software to ensure that only authorized changes are made to company processes and controls.

• Implementation Guidance and Training: As with any significant software application, the users of a Sarbanes-Oxley business process management solution must have guidance and training on both the use of the software and the proper design of business processes and related accounting controls. Without this guidance and training, business process owners may design systems that are perfectly documented and implemented but ultimately fail to comply with Sarbanes-Oxley due to a design flaw.” (M. Ramos http://www.bpmg.org/Zpost977.php)

The Future of SOX 404

2004 was the year in which compliance with Section 404 of Sarbanes-Oxley became required for the first time. One of the initial hurdles in meeting the law’s requirements demanded that companies develop comprehensive documentation of its internal controls. Not surprisingly, the first generation of automated tools were aimed at facilitating the collection, storage and retrieval of information required for compliance. This approach resulted in the creation of a warehouse of control information, separate and distinct from the underlying business process. While these tools achieved the goal of efficiently implementing Section 404, maintaining the existing prototype of manual business processes and a separate store of process documentation will prove to be both inefficient and ineffective in the long run.
Sarbanes-Oxley is not going away any time soon. Company management should seek to implement solutions that provide long-term value. Software applications that manage the company’s business processes building controls “in” rather than bolting them on may prove to be the long term answer companies need.

Impediments to the process of achieving sustainable compliance include:

- **"Project mindset: … many companies understandably treated section 404 compliance as a discrete project with a clearly defined ending point."**

- **"Overextension of internal audit: If management continues to utilize internal audit for intensive 404 and 302 compliance-related work, then a significant infusion of resources (i.e., budget and headcount) to accommodate the additional workload will be needed."**

- **"Poorly defined roles: Internal control-related roles and responsibilities, often poorly defined and segregated from the day-to-day routine of employees during the first year, will require greater clarity and integration going forward"**
"Improvisational approach: Another symptom of deadline pressure showed up in the jerrybuilt practices that carried many companies through the first year."

"Underestimation of technology impacts and implications: …IT is recognized as critical for achieving the goals of the Act, and the impact and implications of technology are widely regarded as significant and pervasive. In many year-one projects, organizations focused heavily on business processes and did not consider the broader role that IT plays in managing financial information and enabling controls. IT will make a huge impact on compliance going forward. At a minimum, technology investments will be necessary to support sustainable compliance in several areas, including repository, work flow, and audit trail functionality. Technology will also be used to enable the integration of financial and internal control monitoring and reporting — a critical requirement at most large and complex enterprises."

"Ignored risks: Effective internal control is predicated on risk. The controls themselves exist expressly for the purpose of minimizing the risk of financial reporting errors. In year one, risk assessment was treated as an afterthought — if addressed at all."

The future of SOX 404 will depend on the ability of businesses to respond to the areas noted above by making it a part of every-day business. Deloitte has developed the "Sustained Compliance Solution Framework":

- Effective and efficient processes for evaluating, testing, re-mediatelying, monitoring, and reporting on controls
- Integrated financial and internal control processes
- Technology to enable compliance
• Clearly articulated roles and responsibilities and assigned accountability
• Education and training to reinforce the "control environment"
• Adaptability and flexibility to respond to organizational and regulatory change.

(Deloitte Touche Tohmatsu, “Under Control”)
The IIA Research Foundation: Sarbanes-Oxley Section 404 Work: Looking at the Benefits. Larry E. Rittenberg (Ernst and Young) & Patricia K. Miller (Deloitte) January 2005


