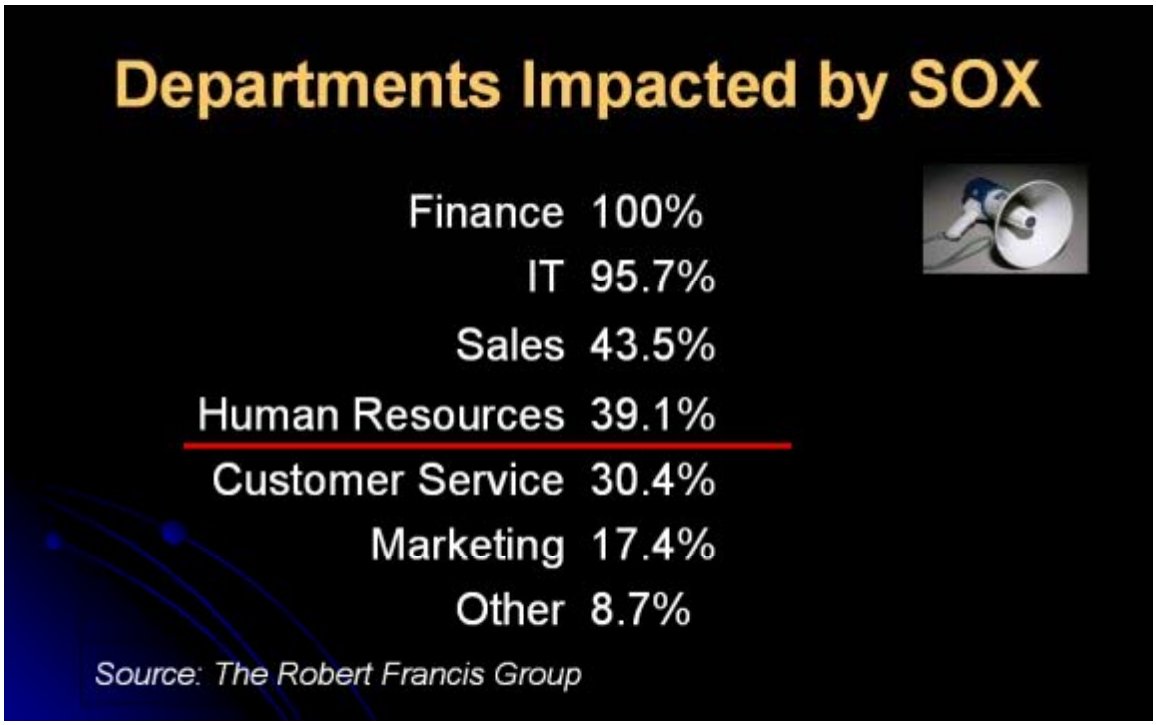
Auditing the Business Continuity Process

Dr. Eric Schmidt, Principal, Transitional Data Services, Inc.

Business continuity audits are rapidly becoming one of the most urgent issues throughout the international community. Recent regulatory initiatives and world events are driving the convergence of business continuity, security and information management under the umbrella of enterprise risk management, sometimes referred to as global assurance. Consequently, financial and technology auditors must review business continuity, and not just disaster recovery, in much more detail than before.



More than cursory reviews are required, as high-level program audits do not address the heightened interest in topics such as disaster preparedness, preventative measures, recovery and restoration of the core business. The question that arises is: "how do you measure business continuity?"

This article will provide background on the Sarbanes-Oxley Act of 2002, prior to discussing the implications for business continuity practitioners.

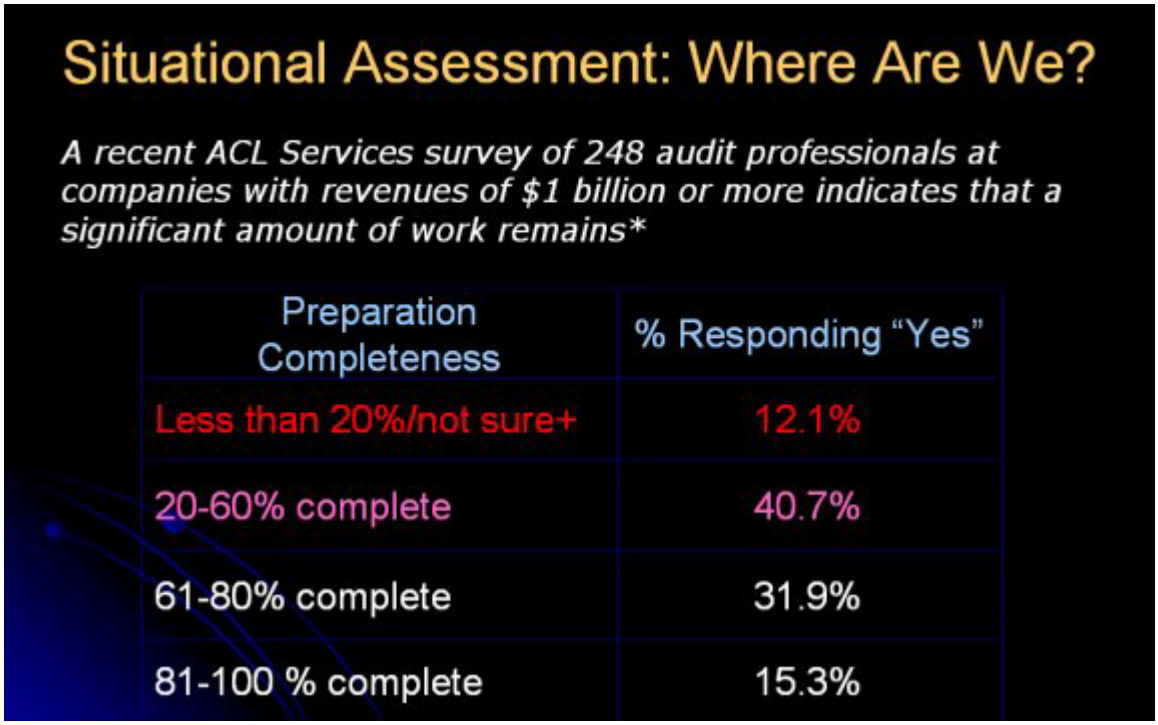
Background

In July of 2002, U.S. Congress passed the Sarbanes-Oxley Act (SOX) mandating that all public companies (SEC registrants) make changes to the way their financial results are reported. This legislation was a response to the high profile failures experienced in the United States and intended to be "a massive restructuring to the regulatory system governing US capital markets" that would improve the quality of financial reporting and disclosures. The Public Company Accounting Oversight Board (PCAOB) was created to oversee the activities of the auditing profession.

The Sarbanes-Oxley Act contains two Sections (302, 404) that deal with management responsibility for controls and one Section (409) on real-time reporting.

Situational Assessment: Where Are We?

A recent ACL Services survey of 248 audit professionals at companies with revenues of $1 billion or more indicates that a significant amount of work remains.*



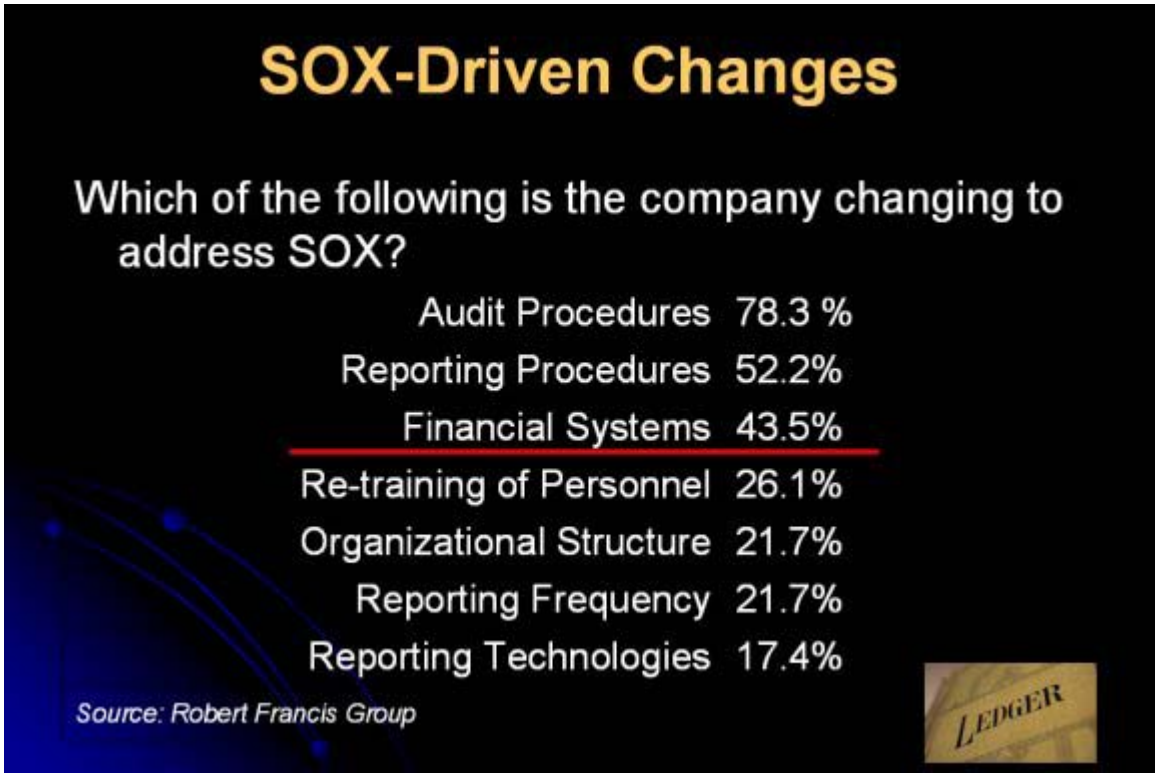
*Source: "Grasping 'Internal Controls'", D. Gullapallia, Wall Street Journal, Nov. 2004

Time to comply with section 404 is running out. Many companies may need to rethink their project timeline—otherwise they are at risk of not complying with the law!

Running Out of Time?

Many companies report that testing and remediation activities are more complex and time consuming than planned. There are several factors contributing:

- Lack of guidance for the number of samples or tests to be conducted,
- Significant numbers of control deficiencies,
- Difficulty in classifying control deficiencies, i.e., internal control deficiency, significant deficiency, or material weakness,
- Insufficient testing of entity-level controls, e.g., the control environment,
- Lack of sufficient and qualified resources to perform the work.



Most audit firms recommend that companies complete testing and remediation activities by the end of the third quarter. By operating on this schedule, the company has sufficient time to test the operating effectiveness of remediated controls. It also provides the independent auditor with time to complete their audit procedures prior to year end.
Implications of not completing testing and remediation activities are significant and include:

- Insufficient time to remediate material weaknesses,
- Adverse opinion on the effectiveness of internal control,
- Negative market reaction,
- Higher cost of capital.

Section 404: Overall Internal Control Effectiveness

Assessment of internal controls consists of two parts:

- Control Design. Management must evaluate the overall effectiveness of internal controls, identify matters for improvement and establish monitoring systems. The control objectives are derived once management maps significant accounts to processes to risks using materiality as a basis.
- Control Effectiveness. Management must ensure an environment of continuous monitoring to maintain the system of internal control and take corrective action in a timely manner.

Section 404 attestation is based on two assessments: (1) adequate documentation of internal controls, and (2) sufficient evidence, e.g., testing. A company must have a framework against which management can make assertions. Hence, the SEC adopted the Committee of Sponsoring Organizations' (COSO) standard, the Internal Control - Integrated Framework (see figure).

COSO is a voluntary private sector organization dedicated to improving the quality of financial reporting through business ethics, effective internal controls, and corporate governance.

COSO was originally formed in 1985 by the National Commission on Fraudulent Financial Reporting, an independent private sector initiative which studied causal factors that can lead to fraudulent financial reporting and developed recommendations for public companies and their independent auditors, for the SEC and other regulators, and for educational institutions.
The National Commission was jointly sponsored by five major financial professional associations in the United States:

- American Accounting Association,
- American Institute of Certified Public Accountants (AICPA),
- Financial Executives Institute (FEI),
- Institute of Internal Auditors (IIA),
- Institute of Management Accountants.

The IT Governance Institute, in conjunction with the Information Systems Audit and Control Association (ISACA) developed a standard for technology, the Control OBjectives for Information and related Technologies (CobiT). This comprehensive framework considers controls from the entity and activity level, thus forming a basis for addressing a variety of business models. Twelve of the CobiT objectives have been closely related with PCAOB's Audit Standard. For more information, visit www.coso.org.

Three Key Aspects of SOX Audit

There are three key areas to consider in any SOX 404 audit. The most significant topic is segregation of duties. It's not just making sure that Accounts Payable and Purchasing staff functions do not overlap. It's important to make sure that IT roles are separate from those of business process owners, specifically those in Finance. This can be a challenge for organizations with few staff members, particularly those who are decentralized.

The second significant topic is change management. It is crucial that an organization have a formal method to gather requirements and specifications from business process owners, including acceptance criteria. Once business and IT are aligned, projects are prioritized, system changes developed, implemented and tested, and then formally released. The process requires a controlled chain of events.

Change management has broad implications, including records and document management, configuration management, business process and controls changes, key reports and even spreadsheets. It spans the spectrum from patch management to mergers and acquisitions.

Audit trail completes the triumvirate. If an organization is weak on segregation of duties or change management, it becomes necessary to perform more audit functions, whether monitoring (preventative) or log-based (detective). Audit trails can quickly become complex and difficult as they must be application-specific, go beyond version control and log files, and must be tamper-proof.

Remediation Challenges

Now that a number of companies have performed their first assessment, they face a number of remediation activities. The most significant of these address:

- Effective decision and governance processes,
- Complex program management initiatives,
- Significant changes to the IT environment,
- Impact on human resources,
- Complex re-testing and roll-forward testing activities,
- Overall need for best practices.

IT clearly has a major role in most of these activities. And the end of the next fiscal year is approaching sooner than one might think.

Does SOX Mandate a Business Continuity Plan? "NO"

According to a statement released by PCAOB in March 2004, a business continuity plan (BCP) is not required for SOX 404 effectiveness. In addition, the AICPA "suspended" the BCP demonstration normally required for a SAS Type 2 audit.

These are temporary measures.

The SAS 70 Type 2 audit is a standard form used by customers to evaluate third-party service providers' controls. However, the information provided on a SAS 70 Type 2 is necessary, but not sufficient to prove compliance, as it leaves the definition of the processes up to the vendor.

What Does "NO" Mean?

Some companies have used the "404 momentum" to address the continuity issue on a broader scale, while others have ignored business continuity entirely. A growing number of executives have been influenced by external auditors who have knowledge of business continuity and potential risks to those companies. As a result, these leaders are concluding they must have business continuity processes, or at least be able to show why they do not have the processes, related to the financial reporting function. Their intent is to extend the assessment to other critical business functions and IT assets at a later date.

The important issue executives now face is to define the scope of the functions and systems necessary to produce timely, accurate, and complete financial reports. Management must make an informed decision and provide guidance to project teams tasked with implementing a continuity solution.

Alignment with Business Continuity

If you look at the twelve CobiT objectives that align closely with PCAOB, you find the basics of a business continuity program. In particular, backup and recovery is a key element, including testing - both on site and off site.

Management involvement and awareness, risk assessment, change management, access rights management, training people and monitoring processes are all common to business continuity and SOX 404.

The role of IT as a pervasive technology, aligned to business goals and objectives during normal operations or operations in abnormal circumstances is still required. And we aren't talking about mythical "best practices", but good practice.

One difficulty to date is testing. How do you test a process that is only performed under abnormal conditions? Formal adoption of business continuity as a requirement for SOX awaits evidence that business continuity professionals have adequately addressed that question.

Success Factors

The most significant factor is sustainability. For a business continuity program to be sustainable, it must be implemented as a business process. Common success factors of sustainable implementations include:

- Enterprise-wide commitment, driven from the top down,
- All managers are knowledgeable and accountable,
- The existence of a dedicated group, staffed with professionals deeply knowledgeable in the business discipline.

Sound familiar? The same success factors that are required for a successful business continuity program operate for SOX and other regulatory requirements. The reason is that all controls and regulations are ultimately derived from process management. And the management and planning of business processes is the heart of business continuity management.

So how do business leaders proceed? A big part of the answer is effective management of information assets. Effective alignment of IT with the business and the reduction of outdated system has a tangible payoff and yields a more resilient organization. It is more cost-effective to deploy a comprehensive program rather than scattered point solutions.

Risk assessments, training, simulation exercises, frequent recovery tests at alternate sites - all of these are prudent. Aside from testing the plan itself, the increased awareness and adoption of the practice of business continuity into the culture of the company is the true win. That's when a state of readiness and preparedness is achieved. Metrics are no longer intangible.

What's Coming Next?

Pundits are calling the start of the new century the "era of compliance." We can expect a ten year cycle of compliance initiatives ahead of us due to regulatory convergence. For example, SOX section 409 goes into effect during 2005. Section 409 focuses on real-time reporting, but is "soft" as (a) no operational definition of material is delineated, (b) it stops short of explicitly requiring disclosure "on the fly" but gives no standard for real-time, and (c) it indicates that SEC rulings after enactment of the statute may guide ongoing interpretation.

So the rules can legally change as the officiating agencies determine their preferred course of action.

We believe that quarterly disclosures and audits will become the norm, in order to achieve the COSO goal of continuous compliance. Expect quarterly scorecards as part of your normal, ongoing practice.

Finally, we believe that there is a confluence of the "axes of assurance" - business continuity, security and information management. The pressures from BASEL II, HIPAA, the Gram-Leach Bliley Act (GLBA), NASD disclosure requirements and SOX are all combining to create the need for core, institutionalized quality management practices that govern resilient organizations.

We, as business continuity professionals, have the responsibility of standing up to show auditors, managers and colleagues how we can help build resilient processes while coping with the pressures of compliance. It's an exciting challenge and one which is energizing our discipline.

About the Author

Dr. Eric Schmidt is a Principal of Transitional Data Services, Inc. (TDS), where he heads the Risk Management and Compliance practice. He has completed projects with over 18 Sarbanes-Oxley customers and 50 Business Continuity customers. Eric has over 110 publications, and is an advisory board member and faculty member at Boston University in the new Emergency Management and Organizational Continuity program.

TDS specializes in IT Orchestration, a customized coordination service that significantly reduces IT management complexity while improving business alignment and the return on IT spending. The four core IT service lines are Strategy and Governance, Design and Implementation, Operations and Support, and Compliance and Risk Management.

Dr. Eric Schmidt, Principal
Transitional Data Services, Inc.
Office: (877) 973-3377, ext 414
Email: eschmidt@transitionaldata.com
www.transitionaldata.com