Technology Facilitates Audit and Compliance: The Sarbanes-Oxley Act Case

By Haralabos Vafiadis, Doctoral Candidate

In the wake of Enron, and other corporate accounting scandals, in 2002, the US government introduced the Sarbanes-Oxley Act of 2002 (SOX). The Sarbanes-Oxley Act of 2002 was an epic legislation and consisted of extensive reforms designed to encourage corporate integrity and accountability, restore public trust, and ensure the independence of the audit profession. Sarbanes-Oxley Act placed a greater-than expected load on public companies regulated by the US Securities and Exchange Commission (SEC), requiring the rapid deployment of large compliance projects. SOX created a services bonanza for auditing and consulting firms to help companies comprehend and meet the SOX requirements. It also created a new software market to provide automated support for SOX compliance requirements.

The initial SOX 404 compliance cycle proved particularly onerous for most firms, revealing a number of challenges and issues that eventually led to lessons learned for future efforts, as well as some reforms in regulatory guidance. The key challenges of the first cycle included:

Inadequate and ambiguous regulatory guidance: The lack of comprehensible regulatory guidance on how to execute the compliance process set many companies in the situation of putting much more effort than was actually necessary. The lack of guidance on the role and relevance of IT systems in the SOX compliance process was a particularly evident omission.

Enormous control costs: The direct costs of the SOX compliance effort included internal resources (e.g., internal auditors and finance personnel), external consultants and external auditors. Causal factors included high external audit fees, inadequate harmonization between externals and internal SOX teams, and necessity to hire expensive external consulting resources to complement internal SOX teams.

Inadequate technology: Companies initially relied on existing in-house tools like Excel to document and evaluate internal controls for SOX compliance. These tools proved inadequate, especially in big firms, due to the large volumes of information and the diversity of file types involved (e.g., text, documents, diagrams, etc.). Acceptance and implementation of purpose-built applications for SOX in the first compliance cycle was limited, due to ambiguous business requirements, and compliance time constraints.

Ineffective financial management systems: Financial management and ERP systems, in many cases, were fragmented, causing complex and time-consuming efforts to close the books and summarize accounting information. SOX compliance process has become a vehicle to make changes in accounting and financial management systems. Firms reacted with efforts to standardize and consolidate accounting and ERP systems, both for efficiency and improved SOX compliance.
The body of knowledge gained in the first SOX compliance cycle has led to clarifications and improved guidance from the regulatory authorities as well as to an emerging set of best practices for internal controls. In April 2005, SEC and the Public Company Accounting Oversight Board (PCAOB) of US issued coordinated guidance to companies and auditors, respectively. The following were part of the key recommendations:

Employ a top-down, risk-based approach: The regulators noted that too many controls were identified, documented, and tested due to a lack of methodical judgment on what was essential. A top-down, risk-based approach ought to be used in order to focus on the areas that have the most material impact on the financial statements. The concept of reasonable assurance was highlighted, to avoid a mechanized approach that goes beyond the scope of what was intended.

Attention should be given to IT controls in the context of financial reporting: The original SOX legislation was unfortunately not detailed on the significance of information technology in financial reporting. In May 2005 regulation acknowledged that IT controls are an important part of the SOX compliance framework, including general IT controls (ITGCs) and application-level controls (ITACs) related to financial reporting. Regulators suggested that not all general IT controls were relevant - only those pertaining to financial reporting. The guidance lacked of a specific IT controls framework and did not clarify which general IT controls were relevant. Many companies have found COBIT to be a useful framework for defining the appropriate IT controls related to SOX

Nowadays as SOX compliance projects mature and software vendors are introducing specific SOX related solutions, technology has become enormously important when managing and optimizing SOX compliance:

ERP systems - the transactional backbone: The core accounting and operational systems, including the general ledger, payment, procurement, receivables, revenue management, and fixed asset management, provide the transactional data hub on which financial reports are based. ERP systems support controls such as authorization and application-level security, as well as producing the accounting information on which financial reports rely. In many cases ERP systems require complex integration and software maintenance and do not encapsulate many of the controls that are needed.

Reporting and consolidation systems - Business Intelligence tools: Accounting systems and ERP systems themselves are usually not sufficient to produce the external financial statements that must be certified for SOX Compliance. Many large public corporations use financial consolidation software to manage the complex aggregation of legal entities, ownership interests, and inter-company transactions.

Controls monitoring and automation software: Controls monitoring and automation takes a variety of different and often complementary approaches, including applications access and segregation of duties controls, transactional data analysis, business controls enforcement, and spreadsheet controls. Today software vendors are putting effort on producing specialized compliance management software applications that achieve a well documented and standardized control framework. These applications should incorporate:

Controls framework: A preconfigured controls framework (i.e., COSO) captures control objectives, risks, and controls details.

Compliance management workflow: Workflow functionality that enables the delegation and execution of task assignments as well as the monitoring of completeness, capturing the necessary sign-offs to finalize the overall evaluation process.

Content and document management: Internal controls documentation will be captured in a variety of forms, including text, process diagrams, questionnaires, reports, and other documents.

Reporting and analysis: Reporting tools and dashboards that will enable the monitoring of the completeness of the compliance effort.

To conclude, although SOX is viewed as a compliance requirement, it is essentially a corporate governance initiative. On a broader scale, corporate governance extends beyond internal controls related to finance and internal audit into IT, human resources, operations, including enterprise risk management (e.g., COSO ERM), quality (e.g., Six Sigma) and IT governance (e.g., COBIT and ITIL). Increasingly, companies will view governance, risk management, and compliance (GRC) as an overarching corporate strategy, with centralized oversight where technology will play a major role.

References

The Sarbanes-Oxley Act of 2002 (Pub. L. No. 107-204, 116 Stat. 745) - a United States Federal Law.
The Public Company Accounting Oversight Board, http://www.pcaobus.org.
http://www.soxlaw.com/
http://www.accenture.com/
http://thecaq.aicpa.org/Resources/Sarbanes+Oxley/
http://www.sarbanes-oxley-101.com/
http://www.aicpa.org/

print out this page