



Sarbanes – Oxley Section 404: Using ScienceLogic’s EM7 to simplify IT related audit tasks

PURPOSE

The purpose of this Whitepaper is not to provide a comprehensive guide to the tasks and responsibilities of IT in a Sarbanes-Oxley (SOX) Audit. Instead, we will provide a broad overview of the types of tasks that are performed as part of a SOX audit and will seek to illuminate ways that these tasks can be automated or simplified.

EXECUTIVE SUMMARY

In 2002 Congress passed the Sarbanes-Oxley Act, legislation which is having significant impact on IT organizations. This legislation, which was passed in response to the corporate scandals of 2001 and 2002, is meant to force executives to vouch for their corporations internal controls and applies not only to internal financial process controls, but to IT related controls as well. Based on Sarbanes-Oxley, financial process controls and IT related controls must now be externally audited and a statement of control must be included with annual reports filed with the Securities and Exchange Commission. These control reports must be personally certified by the companies Chief Executive Officer (CEO) and Chief Financial Office (CFO).

In regards to IT operations although SOX does not specifically mandate technology controls, having these controls will often greatly simplify the compliance process versus a paper-based system. In addition, the logging and audit capabilities of technology controls provide greater confidence in the information presented by these systems.

ScienceLogic’s EM7 System can help companies in their IT control efforts in the six key SOX IT control categories: IS Operations, Network Support, Information Security, System Software Support, Application Systems and Database Support. Through the use of EM7 companies can reduce their management costs in these areas while increasing the availability and accessibility of the data that is used to support a SOX audit.

HOW IT PARTICIPATES IN SOX SECTION 404 COMPLIANCE

Section 404 of the Sarbanes-Oxley Act addresses the ways that corporations maintain the integrity of their financial data. Both the processing and reporting of this data is examined in a SOX audit. Any system, person or processes which influences the integrity of financial data is audited to be sure that proper integrity controls are in place.

The extent of corporate IT systems which may be considered to influence financial data is vast. A sample of systems that may be included in a SOX audit include inventory control, accounts payable, purchasing, accounts receivable, human resources, payroll, order management, payment processing and sales tracking.

According to Deloitte & Touche LLP, a leading SOX Consulting Firm, “Few companies could operate in today’s business environment without complex information systems. In addition to providing critical support to your business, these systems also form a linchpin of your company’s system of internal control. Indeed, IT controls are fundamental to compliance with section 404.”¹

EM7 can help simplify the complexity of ensuring that effective internal controls are in place in today’s complex heterogeneous IT environments.

¹ “Taking Control”, A Guide to Compliance with Section 404 of the Sarbanes-Oxley Act of 2002, Deloitte, 2004, p. 4.

IT CONTROL REQUIREMENTS SUMMARY

In today's IT driven world, the financial data delivered by most companies relies on some form of IT infrastructure to process and store the data. In order to ensure the integrity of the financial data, the integrity of the underlying IT infrastructure must also be considered.

SOX audits will consider the integrity of such things as general IT controls, data controls, application access and owner controls, application integration controls and will even seek to evaluate any third party service providers which may play a role in the delivery of financial data.

In the evaluation of general IT controls the auditor will consider the overall structure and organization of the IT organization. This information will be used to determine the overall organizational attitude towards IT controls. Although this area will normally not be considered as part of a "material deficiency" under SOX, it will be used to guide the auditor throughout the audit. In addition, as part of the audit of general IT controls, the organization will be evaluated to be sure that the management of IT infrastructure supports the integrity of the financial reporting process.

Application access and owner controls will be assessed to ensure that proper access controls are in place for financial reporting related systems. The audit may include evaluation of systems to be sure that access is restricted to those employees whose job duties require that they have access.

Application integration controls will be evaluated to ensure the integrity of data as it passes through several integrated applications. Examples may include the passing of data from an order entry system, to an accounts receivable system, to the system which posts the revenue to the company financial accounts. The security of these integration points as well as the means, by which data integrity is assured, will be examined.

Security controls are a critical part of the SOX audit. Weak security controls can be seen to damage all other areas as data integrity can be compromised by the possibility of unauthorized access.

The above list of audit actions only begins to scratch the surface of the information and processes that a CIO may find themselves having to track (most are discussed in more detail below). The task is so immense that CIO Magazine states "Sarbanes-Oxley compliance efforts are eating up CIO time and budgets. Worse, CIOs are being relegated to a purely tactical role."² The simplification of the IT tasks associated with SOX by ScienceLogic's EM7, is key to a CIO's successful involvement in the SOX process.

² "The SOX Conspiracy", Christopher Koch for CIO Magazine, July 1 2004

IT AUDIT PREPARATIONS

Before undergoing a SOX audit it is essential that a full gap analysis and audit preparation take place. In most companies a SOX team is created with members from various functional areas including IT and Finance. Sub-teams will assess compliance in each of the SOX areas. The IT compliance team should analyze both the general IT infrastructure that handles financial data as well as the applications themselves. The goal of the analysis is to identify gaps in the current systems, people and processes so that they can be remedied.

CLOSING THE GAP

As gaps are identified there will usually be multiple solutions to closing the gap. These solutions may include changing internal policies, creating new or changing current processes or installing new systems. Where possible, the system approach is the most desirable as it is most likely to create the consistency and reliability that is needed to pass the audit. Often, the cost of modifying older paper passed processes is more costly than moving to newer systems based solutions.

USING SCIENCELOGIC'S EM7 TO MEET IT CONTROL REQUIREMENTS

As discussed above, preparation for a SOX audit required companies to examine numerous areas within the company, including system and IT infrastructure. ScienceLogic's EM7 system is designed to help companies more simply manage and understand their IT infrastructure and the data it generates.

When implementing EM7 companies quickly gain new understanding of the applications, systems and infrastructure that supports their financial processes. EM7 can be relied upon as a solution to manage the system-based controls and processes that will be examined during a SOX audit. Using the data produced by EM7 the company, in conjunctions with their external auditors, can identify areas that need improvement and determine the best ways to make the necessary changes.

EM7 can provide assistance in several key IT Control areas. These include:

Security administration: As one of the key areas of IT control, security administration must be verified to allow only the appropriate people access to financial data and related IT assets. During this examination local system users as well as administrators that have access to all systems, must be accounted for. If the proper controls are not in place the integrity of financial reports can not be maintained. EM7 offers numerous features that provide control in this area. At the most basic level EM7 can be setup to detect and alert based on changes in security policies on systems. Alerts can also be generated if new user IDs is created or existing ones removed. Through its port monitoring capabilities EM7 can protect against the installation of "backdoors" on systems by alerting if new ports are opened. Additional EM7 security features include: monitoring of firewalls, monitoring of intrusion detection systems and the ability to verify the patch and hotfix levels installed on systems.

Application Change Management: The ability to monitor what software is installed on key financial systems is extremely important. Changes in the applications or versions of applications installed on key financial systems can make it difficult to maintain control over financial reporting integrity. EM7 provides a simple reporting capability that report installed software and versions. Additionally, the presence of necessary software patches and hotfixes can be monitored through the EM7 software inventory tool. As new software is installed this is cataloged through EM7 so that reports can be generated.

Data Management: The area of data management includes backups, recovery and restoration of data. In order to maintain complete and accurate data the ability to recover data in case of a system failure is paramount. Companies can use EM7 to generate reports on the health and effectiveness of the backup systems that are in place. Alerts can be generated when key systems fail to be backed up or when the performance of the backup infrastructure degrades.

Problem Management: Effective problem management is important to be sure that IT operations provides consistent responses to issues that disrupt IT infrastructure.

Correction of IT infrastructure issues is critical in order to ensure that financial systems are available and performing at required levels. Minimum performance and service levels should be established and monitoring of these service levels should be performed. EM7 provides these capabilities through its integrated trouble ticketing and escalation system. Issues can be categorized by severity and trouble tickets can be automatically escalated by the system to the appropriate levels of management based on committed service levels.

Asset Management: From an IT perspective Asset management for a SOX audit involves being able to account for all IT assets. These assets include hardware and software. Close attention needs to be paid to the proper licensed use of software as significant liability can be created if software licensing terms are not followed. The management of IT assets overlaps heavily with general asset management for other fixed assets within a company. If possible, overall asset management efforts should be coordinated with the efforts within IT. Through EM7's asset management interface companies can track key information about their IT infrastructure. Using the included auto-discovery tool begins the initial population of this data which then can be supplemented to include information such as warranty expiration dates, system owner, etc. In order to facilitate software license compliance EM7 can be queried to determine all systems on which a particular software package is deployed. This list can then be compared to actual licensing to determine any gaps that exist.

OTHER BENEFITS

Establishing strong IT controls and the systems to support these controls provide numerous benefits above and beyond SOX compliance. Companies deploying EM7 report improved efficiency in IT operations, improved customer satisfaction, and reduced costs versus legacy IT control systems. The SOX functionality of EM7 is only a small portion of the power of the overall system. More information can be found at <http://www.em7.com>

CONCLUSION

CIOs can expect a significant amount of work to come from the preparation for a SOX audit. Auditors will expect that a well documented system of processes and controls can be demonstrated. In addition, during the audit it will be expected that the needed data can be easily reached and interpreted. In many cases the implementation of a control system such as ScienceLogic's EM7 may be the most cost-effective and efficient way of meeting the IT control requirements of a SOX audit.

For more information on EM7 please contact your reseller of ScienceLogic directly. More information can be found at <http://www.sciencelogic.com>