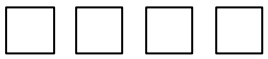
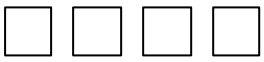


mks

Sarbanes-Oxley and the Need to Audit Your IT Processes

An MKS White Paper

By Jeff Smith
Vice President
Research & Development



Sarbanes-Oxley and the Need to Audit Your IT Processes

Introduction

The Sarbanes-Oxley Act has dramatically heightened standards for financial reporting for US public companies with a market capitalization over $75 million. For the past 18 years, COSO (The Committee of Sponsoring Organizations of the Treadway Commission) has been the accepted framework for implementing internal controls for financial reporting. IT processes and technology, however, are not addressed by COSO. Since the vast majority of financial data that makes up financial reports is generated by IT and its related processes, it is critical that the effectiveness of these processes can be verified. By having well defined standards and procedures that can be verified, CEO's and CFO's can be confident that the reports they are certifying came from well maintained and error free software applications.

The first section of this paper discusses the role that IT will play in complying with the Sarbanes-Oxley Act. We examine the key sections of the Act that IT executives should take most interest in and how they can be at the table when key decisions are made regarding Sarbanes-Oxley.

The second section discusses three popular frameworks or methodologies that can be employed to help establish internal controls for the purpose of complying with Sarbanes-Oxley. We discuss COSO, COBIT and maturity models to illustrate the various approaches to process control and IT governance. They are discussed in descending order of specificity, meaning COSO is represented as the broadest approach to internal controls for financial reporting, while maturity models are detailed methodologies for the self-assessment and benchmarking of processes in the IT realm.

Finally, we introduce the MKS Integrity Solution, a software configuration management and process management solution that can help you achieve reliable process control and repeatability. While COSO defines core financial reporting processes, the MKS Integrity Solution offers internal control of those core processes. SCM software can be implemented to perform version control, ensure process compliance, provide audit trails, automate manual tasks and guarantee the reproducibility of software applications. The MKS Integrity Solution itself will not guarantee compliance with Sarbanes Oxley, but it can perform a valuable function in ensuring IT processes are disciplined and controlled.

1. The Sarbanes-Oxley Act

The Sarbanes-Oxley Act was enacted on July 30, 2002 in response to a number of major corporate accounting scandals that rocked the American business landscape. The scandals resulted in a loss of public trust in financial reporting and accounting practices and required immediate attention from legislators who recognized that, if left unaddressed, the loss of trust could have deepened to a system wide malaise. The Act, therefore, was meant to prevent future accounting scandals and rebuild the trust of the investing public.

Sarbanes-Oxley creates new or enhanced standards for corporate accountability and penalties for corporate wrongdoing. It contains 11 titles setting out auditor and corporate responsibilities, rules for financial disclosures and harsher penalties for white collar crimes. The two sections that should concern IT executives the most are 302 and 404(a) because they deal with the internal controls that a company has in place to ensure the accuracy of their data. This relates directly to

the software systems that a company uses to control, transmit and calculate the data that is used in their financial reports.

Section 302

Effective August 29, 2002, Section 302 requires CEO's and CFO's to attest to the accuracy of their company's quarterly and annual reports. They must certify a number of representations listed below:

1. They have viewed the report.

2. To the best of their knowledge, the report contains no untrue statement of a material fact and does not omit any material fact that would cause any statements to be misleading.

3. To the best of their knowledge, the financial statements and other financial information in the report fairly present, in all material aspects, the company's financial position, results of operations and cash flows.

4. They accept responsibility for establishing and maintaining disclosure controls and procedures, and the report contains an evaluation of the effectiveness of these measures.

5. Any major deficiencies or material weaknesses in controls, and any control-related fraud, have been disclosed to the audit committee and external auditor.

6. The report discloses significant changes affecting internal controls that have occurred since the last report, and whether corrective actions have been taken.

Due to the potential civil and criminal penalties involved, CIO's and IT executives should be concerned with Section 302. CEO's and CFO's will be placing an enormous amount of trust in the people and systems that produce their company's financial data. Given and wide and deep spectrum of internal controls, it is a serious responsibility.

Section 404(a)
The deadline for complying with this rule was originally September 15, 2003, but it was recently extended to June 15, 2004. A number of experts view the extension as a sign of just how seriously authorities intend to enforce and monitor the new law. Check the SEC website for their June announcement on compliance dates for Section 404 (http://www.sec.gov/rules/final/33-8238.htm) because there are some variances.

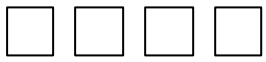
Because the SEC oversees the financial reporting process, they were given the responsibility of defining the rules for this particular section of Sarbanes-Oxley. The SEC, therefore, proposed a rule that would require each annual report issued by a company under the Exchange Act to contain an internal control report that:

- States management's responsibility for establishing and maintaining adequate internal control over financial reporting for the company;
- Identifies the framework used by management to evaluate the effectiveness of this internal control;
- Assesses the effectiveness of this internal control as of the end of the company's most recent fiscal year; and
- States that its auditor issued an attestation report on management's assessment.

In the same June, 2003 announcement mentioned above, the SEC recognized the COSO framework as the official framework for establishing internal controls over financial reporting. They said, "We recognize that our definition of the term 'internal control over financial reporting' reflected in the final rules encompasses the subset of internal controls addressed in the COSO Report that pertains to financial reporting objectives." If you have not already spoken to your external auditors to set expectations about Section 404, it would be wise to do so to avoid unwanted surprises next year when Section 404 comes into full force.

i) The View From the Top

Understandably, CEO's and CFO's are taking Sarbanes-Oxley very seriously given the potential penalties for non-compliance. There is a tremendous amount of data that they will have to monitor to make sure the financial statements are accurate. From the point of view of an IT person, it is a given that IT will be relied upon to collect, store and compile this data from all areas of the company and transmit it to the appropriate people.



So, how do CEO's and CFO's view Sarbanes-Oxley from a compliance standpoint? Surprisingly, an informal survey by CIO Magazine of the top 19 companies on the Fortune 100 list revealed that most executives viewed compliance as a finance issue, not a systems issue[1]. This is a mistake, as IT is poised to play a major role in the implementation of controls for financial reporting.

ii) What Sarbanes-Oxley Means to IT Executives

Sarbanes-Oxley offers you the opportunity to take a seat at the inner table with top executives as you sell the merits of IT's participation in regulatory compliance. According to CIO Magazine, CIO's must be proactive in getting the attention of their CFO's so that they understand how important IT systems are to data integrity. One way to do this is by demonstrating a detailed understanding of Sarbanes-Oxley and the part you can play in achieving compliance – without claiming that IT holds all the answers. Seats at the inner table, "are usually reserved for CIOs who can explain the business value of technology changes, but who are also able to put on their business hat and review potential IT work in the context of the broader business needs."[2]

From a departmental perspective, be prepared for greater audit scrutiny. The financial reporting process depends heavily on internal software systems to generate and transmit the necessary financial data. IT processes, therefore, can be considered an "internal control" that must be audited to ensure compliance with the law and, equally important, that they are secure, comprehensive and repeatable. The benefits of such an audit extend beyond compliance with the law to the overall quality and reliability of your company's systems. This, and the June 15, 2004 deadline, should be incentive enough to start the auditing process now.

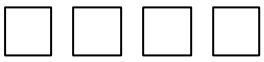
The second section of this white paper examines some of the methodologies and tools that are currently available to assist your organization's process control and auditing capabilities.

2. IT Governance and Auditing

The pervasiveness of IT in today's business environment points to its potentially critical role in regulatory compliance, especially Sarbanes-Oxley. This includes software and hardware, but more importantly the processes that govern their use. Luckily, there are some good methodologies and guidelines that already exist to help bring your IT processes under control so they are ready to be audited. ISO 9000 is a well known generic management system standard, which means it is concerned with the way an organization goes about its work, and not directly the result of this work. This standard can be applied to any organization, large or small, whatever its product or service in any sector of activity, including business, public administration, or government. If you consider financial reports as internal end products, then ISO standards can be helpful for achieving a high level of quality, but they do not specifically address financial reporting or IT processes. For that, frameworks specially designed for these purposes should be consulted.

The three frameworks, or methodologies, discussed below are a good starting point for these efforts. COSO, as mentioned, is a framework for establishing internal controls over financial reporting. COBIT is an IT governance frameworks that can be applied to the entire IT realm and

[1] Ben Worthen, *Playing by New Rules – Sarbanes-Oxley: Your Risks and Responsibilities*, May 15, 2003, CIO Magazine
[2] *Playing by New Rules*, p. 6



its processes in general, and maturity models represent a more detailed and granular approach to controlling individual processes within the IT realm. While there are guidelines, there are no "one-size-fits-all" frameworks. The three frameworks and methodologies are listed below in descending order of granularity with regards to specific process control activities.

a) COSO – When speaking of Sarbanes-Oxley, COSO usually comes up as the leading framework in this area, especially after the SEC's June, 2003 announcement recognizing it as its preferred framework. COSO (The Committee of Sponsoring Organizations of the Treadway Commission) was established in 1985 to sponsor the National Commission on Fraudulent Financial Reporting. The Commission was an independent private sector initiative which studied the 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.

COSO issued a groundbreaking report entitled *Internal Control – Integrated Framework* in 1992, which identified the establishment of internal controls as a means for helping a company achieve numerous objectives. The objectives include achieving its performance and profitability targets, preventing loss of resources and ensuring reliable financial reporting. The reason this report has become entwined with Sarbanes-Oxley is its assertion that internal controls help ensure that the company complies with laws and regulations, avoiding damage to its reputation and other consequences. Many companies used this report as the basis for their immediate response to Sarbanes-Oxley.

In July, 2003, COSO is scheduled to release the most comprehensive update of its 1992 report. It incorporates and expands on the 1992 report to address Enterprise Wide Risk Management (EWRM). The new framework emphasizes the importance of identifying and managing risks across the enterprise. According to one expert organization that has seen advance copies of the framework, COSO's new ERM framework consists of eight components: internal environment, objective setting, event identification, risk assessment, risk response, control activities, information and communication, and monitoring. The three new components of the COSO framework are objective setting, event identification, and risk response. And the five taken from the control model are broader in their descriptions and in terms of the practical guidance.[3]

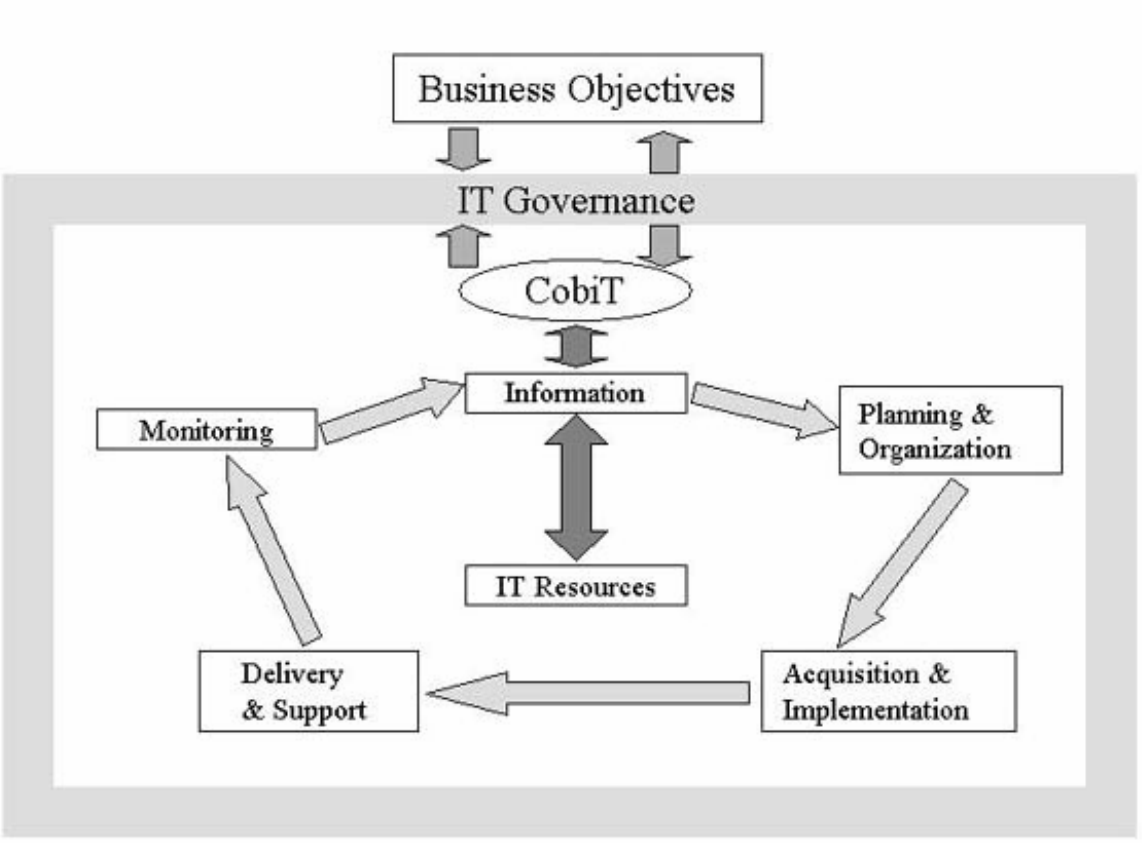
COSO and its findings are mentioned often in conjunction with Sarbanes-Oxley because of the role it has played in establishing financial reporting controls, yet it is only a guide for the entire organization and offers little about how IT organizations, in particular, can meet their unique challenges. The following frameworks represent the actual processes that IT organizations can use to establish effective internal controls in preparation for IT audits.

b) COBIT – COBIT (Control Objectives for Information and Related Technology) was developed by the IT Governance Institute as a generally applicable and accepted standard for good Information Technology (IT) security and control practices that provides a reference framework for management, users, and IS audit, control and security practitioners. The institute was founded in 1998 by the Information Systems Audit and Control Association (ISACA) as a not-for-profit organization dedicated to sharing better practices for IT governance,.

[3] D'Arcangelo & Co.,LLP, Certified Public Accountants (D'Arcangelo Software Services website) http://www.darcangelosoftwareservices.com/media/inthenews/COSO_update.htm

According to COBIT, IT governance is a structure of relationships and processes to direct and control the enterprise in order to achieve the enterprise's goals by adding value while balancing risk versus return over IT and its processes[4]. It provides the structure that links IT processes, IT resources and information to enterprise strategies and objectives.

COBIT's framework for IT governance identifies 34 key, naturally grouped IT *Control Objectives*, which fall under one of four broad domains: planning and organization (11), acquisition and implementation (6), delivery and support (13), and monitoring (4). Each control objective can be regarded as a separate process to which COBIT's *Management Guidelines* are applied. The management guidelines are governed by a generic maturity model that allows managers to map where the organization is today, where it stands in relation to the best-in-class in its industry and to international standards and where the organization wants to be. The following section discusses maturity models, and in particular the Software Capability Maturity Model, as a means for controlling software development processes.



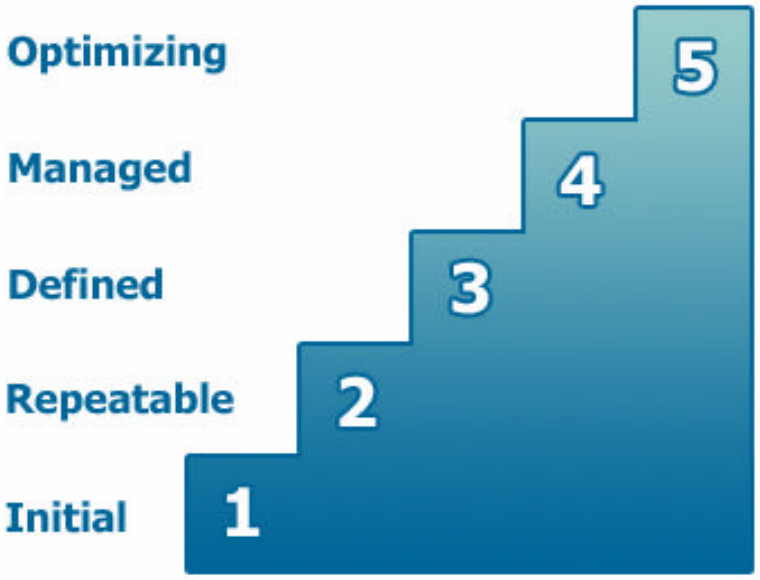
Source: ISACA

As it relates to Sarbanes-Oxley, COBIT represents an excellent reference point for assessing current internal process controls and implementing new and improved ones. An IT governance

[4] COBIT 3rd Edition – Executive Summary, July 2000, p. 3.

model such as this is a worthy goal to aspire to in the longer term, but to comply with the Act, more immediate and short term actions can and should be taken.

c) Maturity Models - Like any business process, IT processes lend themselves to auditing activities that track their effectiveness in achieving business goals. Key to this measurement is the use of maturity models for self-assessment and benchmarking. Maturity models are effective tools for determining the current status of the organization's processes and how they should evolve. They provide both the goals to strive for and the means of measuring the attainment of those goals. If you are planning to audit your IT processes, they provide one of the readiest and effective tools for preparing for it. There are five levels that make up the generic maturity model:



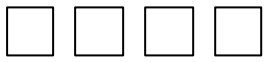
Generic maturity model levels – Source: Software Engineering Institute

The Capability Maturity Model (CMM)

To understand how maturity models are applied in the real world, consider the example of software development processes. For a number of years, software development organizations have used the Capability Maturity Model for Software (SW-CMM) as the de facto standard for assessing and improving software processes. Developed by the software community under the stewardship of the Software Engineering Institute (SEI) at Carnegie Mellon, it describes the principles and practices underlying software process maturity and is organized into the same five maturity levels as the generic model:

1) Initial - Software processes are ad hoc. There are few defined processes and success depends on individual effort.

2) Repeatable - Basic project management processes are established to track cost, schedule, and functionality. The necessary process discipline is in place to repeat earlier successes on projects with similar applications.



3) Defined - The software process for both management and engineering activities is documented, standardized, and integrated into a standard software process for the organization. All projects use an approved, tailored version of the organization's standard software process for developing and maintaining software.

4) Managed - Detailed measurements of the software process and product quality are collected. Both the software process and products are quantitatively understood and controlled.

5) Optimizing - Continuous process improvement is enabled by quantitative feedback from the process and from piloting innovative ideas and technologies.

3. Using the MKS Integrity Solution For Process Control and Auditing

One of the main goals of Sarbanes-Oxley is to improve companies' internal control over financial reporting. The MKS Integrity Solution provides control over IT processes to make them more verifiable and auditable. Software configuration management and process management tools offer an effective way of controlling IT processes at a modest price. SCM was designed to provide assurance that a company's mission critical software applications are not exposed to potential failure due to human error, staff turnover or sabotage. As SCM has become better understood and applied in different areas, however, a secondary but important role has emerged. SCM, in conjunction with a flexible process and workflow management solution, provides the ability to capture, track, version and report on changes to any process or system in an IT setting.

The award-winning MKS Integrity Solution can help you bring your IT processes under control, so they are audit-ready for Sarbanes-Oxley. If you are using a maturity model to assess and measure the evolution and progress of your processes, the MKS Integrity Solution can help because many of our customers who use it for software development have used it to achieve CMM level 2 and beyond.

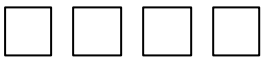
MKS Integrity Manager

MKS Integrity Manager is a flexible process and workflow management solution that allows you to implement workflows that are customized for any IT process or system. It records every change and/or action made by every person involved in a given process, providing valuable details about "who's done what". The workflows are completely enforceable, meaning that a process cannot be subverted by an overzealous or malicious employee who wishes to skip steps in the process.

Go/no-go gates are the mechanisms that provide managers with the ability to enforce workflows and decide when the process can proceed and when it must remain stopped until another person in the process completes his/her action. Finally, MKS Integrity Manager comes with a graphical workflow modeler to make for easy graphical editing of workflows while providing a clear overall picture of the people and actions involved.

MKS Source Integrity Enterprise Edition

MKS Source Integrity Enterprise Edition is a cross-platform software configuration management solution that provides traditional SCM functionality, and much more. It plays a central role in software development with its ability to version any type of file, guarantee the reproducibility of



an application, and provide audit trails for illustrating migrations throughout the software development process.

MKS Source Integrity Enterprise provides value for Sarbanes-Oxley compliance through its versioning capabilities and its integration with MKS Integrity Manager. In a typical company, processes and workflows are defined and documented, and implemented, in that order. MKS Integrity Manager allows you to implement and enforce those processes, while MKS Source Integrity Enterprise performs the versioning of the process documents. This is not a trivial task. As processes improve and evolve, process documents will undergo almost constant revision. In an audit situation, a separation of duties and clear audit trail must be evident to illustrate that IT processes are up to date and in synchronization with what is being practiced by staff. An audit trail of approvals is also critical for demonstrating that internal controls are working properly.

4. Conclusion

A disciplined approach to internal process controls and good IT governance are the keys to complying with Sarbanes-Oxley. Section 404(a) calls on companies to identify the framework used by management to evaluate the effectiveness of their internal control and then to attest to the effectiveness of these controls in the year end financial report. This paper discussed a framework, COSO, that can be used to establish internal control over financial reporting. COBIT and maturity models, such as the Capability Maturity Model for software, are methodologies for establishing good IT governance practices and assessing and measuring the effectiveness of IT processes.

An SCM and process and workflow management solution, such as the MKS Integrity Solution, will complement your compliance efforts by recording, managing, enforcing and auditing the IT processes that form your internal control mechanisms.

Helpful Online Resources

The Committee of Sponsoring Organizations of the Treadway Committee (COSO) - http://www.coso.org/

The Information Systems Audit and Control Association & Foundation (ISACA) - http://www.isaca.org

IT Governance Portal – http://www.itgovernance.org/

Sarbanes-Oxley Information Center – http://www.sarbanes-oxley.com

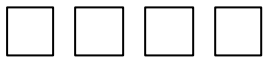
United States Securities and Exchange Commission – http://www.sec.gov/index.htm

PWC's CFO Direct Network (Sarbanes-Oxley Info Center) – http://www.cfodirect.com

Carnegie Mellon SEI (SW-CMM) – http://www.sei.cmu.edu/cmm/cmm.html

KPMG's Audit Committee Institute – http://www.kpmg.com/aci/gov.htm

MKS Inc. – www.mks.com



References

Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Internal Control – Integrated Framework, Volumes I &II*, American Institute of Certified Public Accountants (AICPA), 1992.

Comrie, George R., *Software Development is Risky Business – Is it Audit Ready?*, 2001, ISACA InfoByte - ISACA Website.

International Organization for Standardization, *Demystifying ISO 9000 and ISO 14000*, ISO Website - http://www.iso.ch/iso/en/iso9000-14000/tour/magical.html

Thomke, Stefan, *R&D Comes to Services: Bank of America's Pathbreaking Experiments*, Harvard Business Review, April, 2003.

IT Governance Institute, *COBIT 3rd Edition – Executive Summary*, July, 2000.

IT Governance Institute, *COBIT 3rd Edition – Management Guidelines*, July, 2000.

KPMG, *Sarbanes-Oxley Section 404: Management Assessment of Internal Control and the Proposed Auditing Standards*, March 2003.

MacSweeney, Greg, *Governance Falls Into CIO's Lap, Wall Street & Technology Online*, May 29, 2003.

PriceWaterhouseCoopers, *Navigating the Sarbanes-Oxley Act of 2002 – Overview and Observations*, March, 2003.

PriceWaterhouseCoopers, *The Sarbanes-Oxley Act of 2002: Strategies For Meeting New Internal Control Reporting Challenges*, 2002.

Worthen, Ben, *Playing By New Rules – Sarbanes-Oxley: Your Risks and Responsibilities*, CIO Magazine, May 15, 2003.