The Emerald Research Register for this journal is available at
www.emeraldinsight.com/researchregister

The current issue and full text archive of this journal is available at
www.emeraldinsight.com/0968-5227.htm

What ERP systems can tell us about Sarbanes-Oxley

William Brown
Minnesota State University, Mankato, Minnesota, USA, and
Frank Nasuti
The Institute for Internal Controls, Inc., Laurel Springs, New Jersey, USA

Abstract

Purpose – To provide background for senior and middle management in information technology organizations who may be in the implementation phase of compliance for Sarbanes-Oxley (SOX). As the information technology (IT) organization looks forward to additional compliance or other IT control frameworks such as COBIT, the paper can help construct a roadmap. Other audiences include senior management, accountants, internal auditors, and academics who may wish to evaluate the impact of SOX on the information technology organization.

Design/methodology/approach – SOX is surveyed to understand the four major compliance areas that must be supported in the IT organization. Recently published works are integrated into an evaluation of enterprise resource planning (ERP) research to identity several ongoing themes that point to practical advice for implementing SOX. The private sector of US business is saturated with ERP applications and provides a useful benchmark of what to expect with SOX compliance. The sections of this report include: SOX and IT governance; ERP systems: recurring themes; after the initial implementation of SOX; frameworks to support SOX compliance; IT governance and SOX: where we go from here; to best practice and competitive advantage; and conclusion.

Findings – Competencies in several related core disciplines including project management, change management, and software integration should be the top priority for SOX implementation. Enterprise architecting and related areas such as security and outsourcing can be managed more effectively with the appropriate competencies.

Research limitations/implications – The authors' observations are based on several research reports but are not exhaustive, and are not specific to a particular industry.

Originality/value – The content is a very useful source of information for senior management, IT management, accountants, auditors, and academics to understand the impact of SOX on the IT organization and how to develop a roadmap to respond.

Keywords Manufacturing resource planning, Communications technologies

Paper type Literature review

Introduction

In response to the series of business failures and corporate scandals that began with Enron in 2001, the US Congress enacted the Sarbanes-Oxley (SOX) Act of 2002. The stated purpose of SOX is to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws (PCAOB, 2002). The duties of the chief executive office (CEO), the chief financial officer (CFO), and the auditor are outlined by SOX, including making each personally responsible for ensuring the credibility of the financial reporting provided to stakeholders. There are 11 sections of SOX defining auditor and corporate responsibilities, including expectations for financial disclosures, strong penalties for white-collar crimes, and protection for "whistleblowers" (PCAOB, 2002).

Information Management & Computer Security
Vol. 13 No. 4, 2005
pp. 311-327

0968-5227
DOI 10.1108/09685220510614434

SAP (2005) reports that 80 percent of the *Fortune* 500 firms have implemented some form of enterprise resource planning (ERP) system and concludes that the private sector market for ERP is saturated. An ERP system is defined by Deloitte & Touche (1999) as a packaged business solution that is designed to automate and integrate business processes, share common data and practices across the enterprise, and provide access to information in a real-time environment. Deloitte & Touche require an ERP system:

- have real-time access to the same data;
- integrate business processes fully (i.e. position-based budgeting sees the human resources data, customer relationship management sees and posts to live inventory data for orders); and
- enable users to move seamlessly from one function to another.

A report by Computer Economics, Inc. states that 76 percent of manufacturers, 35 percent of insurance and health care companies, and 24 percent of federal government agencies already have ERP systems or are in the process of installing them (Hawking *et al.*, 2004). SAP reports that the public sector and medium- to small-sized firms in the private sector remain growth sectors for the future.

With over 80 percent of the *Fortune* 500 using ERP applications, enterprise architecting and performance issues in areas such as change management and process engineering can pose primary or secondary risks to financial information. SOX requires ongoing risk management of the processing environment and casts ERP systems into a central collection role of risk management data for the enterprise. Supply chain management (SCM), customer relation management (CRM) systems, and new e-business applications are frequently integrated into ERP systems and further complicate SOX compliance. The purpose of this paper is to examine enterprise systems that are dominated by ERP applications and to examine SOX compliance.

This paper will discuss:

- the basic concepts of SOX;
- Control Objectives for Information and Related Technology (COBIT), a generally accepted framework for IT auditors who map to SOX requirements (Chan, 2004; Ramos, 2004); and
- other frameworks to facilitate SOX compliance as well as the value they can add to the IT organization.

Many CIOs may be asking whether COBIT is a necessary step to migrate to SOX compliance. While SOX compliance is necessary for a publicly traded company, application development (e.g. SCM and SCM) adds the most value to a company's competitive and strategic advantage (Luftman *et al.*, 2004). The frameworks adopted for SOX or COBIT should contribute to the strategy, architecture, and the planning processes to further enable the information technology (IT) organization to manage, anticipate, and assemble technologies and methodologies to ensure a stable and continuously improving IT environment. A stable and continuously improving IT environment should contribute to application development and a company's competitive and strategic advantage.

SOX and IT governance

Key sections of SOX compliance that directly involve IT include Sections 302, 404, 409, and 802 (PCAOB, 2002). Section 302 requires the officers of the company to make representations related to the disclosure of internals controls, procedures, and assurance from fraud. Section 404 requires an annual assessment of the effectiveness of internal controls. Section 409 requires disclosures to the public on a "rapid and current basis" of material changes to the firm's financial condition. Section 802 requires authentic and immutable record retention. As a change agent, the Securities and Exchange Commission (SEC) is very effective and will assert itself in the future if these four sections or other sections require additional compliance measures (Mead and McGraw, 2004). The SEC has effectively imposed requirements for SOX on senior management and simultaneously aligned the same requirements on the CIO and the IT organization.

The scope of impact is not limited to the CEO, CFO, and auditor, nor is it limited to SEC registrants (i.e. public companies). More and more of SOX's provisions are becoming applicable to private companies as well (Heffes, 2005). More and more lenders and states are asking private companies about the status of their internal control environments.

While the CEO and the board of directors are accountable for overall corporate management, SOX also impacts on the IT administration, including organization governance, the responsibilities of CIOs, budgets, vendors, outsourcers, and business continuity plans. Among the most widely hyped, in terms of impacts, are reporting content and the timeliness of reports (Garretson, 2003; Marlin, 2003). CEOs and CFOs require their IT organizations to provide them with proof that automated portions of financial processes have appropriate controls, computer generated financial reports are accurate and complete, and any exceptions are being captured and reported to them in a timely manner (Kaarst-Brown and Kelly, 2005).

Section 302

Recent surveys of CIOs report that 44 percent of the companies will require the CIO to certify financial results under SOX compliance (CIO Insight/Gartner, 2004). Gartner and various CIO journals have suggested the SEC may eventually require the CIO to sign a statement in the annual report attesting to the effectiveness of controls and the accuracy of the financial reports (CIO Insight/Gartner, 2004). Because of the significance of information prepared by others, it is becoming common for the CEO and CFO to request those individuals who are directly responsible for this information to certify it. This process is known as sub-certification, and it usually requires the individuals to provide a written affidavit to the CEO and CFO that will allow them to sign their certifications in good faith (Ramos, 2004). Items that may be the subject of sub-certification affidavits include a statement of accuracy of specific account balances, compliance with company policies and procedures, the company's code of conduct, and the adequacy of the design and/or operating effectiveness of internal controls.

Whether the reported 44 percent will increase or decrease over time remains to be seen. In-depth interviews with over 50 CIOs in the USA and Canada determined that rapid strategic business change and e-business and technology complexity will be significant drivers in the near future (Reich and Nelson, 2003). As organizations

transition into more e-business and more architectural complexity, it is reasonable to assume that the 44 percent may increase to meet SOX compliance.

Section 404

Section 404, in conjunction with the related SEC rules and Auditing Standard No. 2 established by the Public Company Accounting Oversight Board (PCAOB) (2005), is driving pervasive change in the internal controls of the enterprise and requires the management of a public company and the company's independent auditor to issue two new reports at the end of every fiscal year (PCAOB, 2002). These reports must be included in the company's annual report filed with the SEC. The internal control report must include:

- A statement of management's responsibility for establishing and maintaining adequate internal control.
- Management's assessment of the effectiveness of the company's internal control.
- A statement identifying the framework used by management to evaluate the effectiveness of the company's internal control.
- A statement that a registered public accounting firm audited the company's financial statements included in the annual report.
- An attestation report on management's assessment of the company's internal control over financial reporting.

Under Section 404, management must also disclose any material weaknesses in internal control. If a material weakness exists, management may not be able to conclude that the company's internal control over financial reporting is effective (PCAOB, 2002). These management statements are not enough, however; the company's auditor must also attest to the truthfulness of these management internal control assertions.

The Committee of Sponsoring Organizations (COSO) of the Treadway Commission recommended the enterprise risk management – integrated framework (ERM) to manage and reduce risks, to be applicable to all industries, and to encompass all types of risk (COSO, 2005). Moreover, the ERM framework recognizes that an effective enterprise risk management process must be applied within the context of strategy setting. ERM is fundamentally different from most risk models used in that it starts with the top of the organization and supports the organization's major mission (COSO, 2005; Louwers *et al.*, 2005).

The COSO framework describes five interrelated components of internal control in Section 404. The CEO and the CFO in concert with the CIO are responsible for (Ramos, 2004):

- "tone at the top" that positively influences the attitude of the personnel;
- identification of risks, objectives, and the methods to manage the risks;
- activities and procedures that are established and executed to address risks;
- information systems to capture and exchange the information needed to conduct, manage, and control its operations; and
- the monitoring of and responses to changing conditions as warranted.

COSO creates a framework that divides IT controls into two types (Ramos, 2004):

(1) general computer controls; and
(2) application-specific controls.

General controls include:

- data center operations (e.g. job scheduling, backup and recovery);
- systems software controls (e.g. acquisition and implementation of systems);
- access security; and
- application system development and maintenance controls.

Application controls are designed to:

- control data processing;
- ensure the integrity of transactions, authorization, and validity; and
- encompass how different applications interface and exchange data.

The ERM framework, a cornerstone of Section 404 and COSO, requires ongoing feedback of information from throughout the company. This information must be current and accurate and must be sufficiently robust to support the analysis of different risk responses (COSO, 2005). ERP systems and integrated systems must have the highest levels of integrity and controls. Enterprise risk management cannot be effective if the technology that provides the data used to manage the enterprise risk are flawed, corrupted, or not available. Many firms are implementing risk management applications to assist with internal control and assessment processes (Decker and Lepeak, 2003). A main objective of these tools is to lower external audit verification costs. Consistent with that objective, tools that have more automation and tighter integration with ERP processes are favored.

The ongoing assessment of Section 404 requirements requires a critical evaluation of legacy processes including ERP, operational, and off-line management processes. An ERP SOX solution for financial and operational areas will be critical for a company that has moved to consolidated financial and operational processes (Decker and Lepeak, 2003). ERP centered risk management applications (e.g. Oracle Internal Controls Manager, PeopleSoft Enterprise Internal Controls Enforcer, SAP), as well as solutions that have effective integration with ERP (e.g. Movaris), have pre-built diagnostic tools to test and continuously monitor configuration changes. The opportunities for corruption of transactional data include the timing of interface-validation tables, manual intervention, and overlap of security rights. Firms must continually assess operational processes such as SCM and CRM that drive financial transactions and the risks associated with those transactions. Self-assessment processes where managers can certify that the appropriate review/corrective actions are taken must be directed to the broken operational processes (e.g. SCM and CRM) that can correlate with broader financial risk for the enterprise.

Section 409

Section 409 requires that organizations disclose to the public on a rapid and current basis, material changes to a firm's financial condition (PCAOB, 2002). An example of a

Section 409 compliance consideration for IT would be a situation where a computer virus knocks out the supply chain and materially affects the financial performance of a quarterly financial report (Proctor, 2004). This would be a discloseble event for financial reporting purposes under SOX.

Section 802

The IT organization must have policies in place to ensure appropriate record retention and security. SOX has a direct impact on data management, data and system security, and business recovery practices (PCAOB, 2002). The CIO must understand the requirements, and ensure that the appropriate policies are in place including ongoing compliance.

ERP systems: recurring themes

Competencies

Deloitte & Touche (1999) conducted in-depth interviews with 164 individuals at 62 *Fortune* 500 companies that used ERP systems such as SAP, Baan, Oracle, and PeopleSoft. The purpose of the study was to evaluate ERP development issues. The study summarized performance problems into three categories:

(1) people: 62 percent;

(2) business process: 16 percent; and

(3) IT: 12 percent.

A report from Deloitte Consulting (1999) reported similar results (Table I).

Consistent with the reports from Deloitte, Benesh (1999) described five areas of common management pitfalls that involve:

(1) shortcomings in or a lack of integrated project team planning;

(2) managed communications across many people;

(3) formal decision-making processes;

(4) integrated test plans and managed test processes; and

(5) the failure to integrate lessons learned into current practice.

Barrier	Category
Lack of discipline	People
Lack of change management people	People
Inadequate training	People
Poor reporting procedures – technical	People
Inadequate process engineering	People
Process misplaced benefit ownership	People
Inadequate internal staff	People
Poor prioritization of resources	People
Poor software functionality	Technical
Inadequate ongoing support	People
Poor business performance	Process
Underperformed project team	People
Poor application management	Technical

Table I.
ERP barriers focus

In a survey of critical success factors throughout all stages of ERP implementations in 86 companies, factors similar to those reported by Benesh and Deloitte were ranked high in importance (Somers and Nelson, 2001). Those factors included project team competence, project management, vendor support, package selection, data analysis and conversion, and business process reengineering. In-depth interviews with over 50 CIOs produced a similar theme: project management and process engineering skills were frequently mentioned as shortcomings in the course of enterprise development (Reich and Nelson, 2003).

Design and implementation of enterprise architecture

CIOs cite problems with data structures, difficulties ensuring adequate security and business continuity, and variations in infrastructure between business units as three of the top four obstacles to SOX compliance (Ziff Davis, 2004). Many of the issues are the results of years of building information systems one-by-one in complex organizations, where data definitions, business rules and operating procedures are determined separately by each department.

ERP projects have been plagued by complex technical problems (Krasner, 2000), which fall into the following general categories: non-robust and incomplete ERP packages, complex and undefined ERP-to-legacy-system interfaces, middleware technology bugs, poor custom codes, and poor system performances. Chang *et al.* (2000) identify ten major issues in the implementation of SAP ERP systems in their research. Among the significant findings are that 52 percent of surveyed individuals refer to issues in system development and 49 percent nominated operational deficiencies as major issues. Both of these responses are directly related to enterprise architecture.

In a survey by the META Group, the top preferences for SOX solutions reflect a resolution of chronic ERP problems. The top SOX solutions included (Lepeak, 2004):

- replace ERP solution: 2 percent;
- consolidate ERP applications: 6 percent;
- move from point solutions to ERP applications: 7 percent;
- upgrade to latest version of ERP application: 8 percent;
- turn on existing ERP functionality: 11 percent;
- evaluate/implement business process management: 15 percent;
- evaluate/implement internal SOX compliance dashboards: 15 percent.

E-business requirements will make significant changes in enterprise systems in the near future and may complicate existing problems in enterprise installations (Reich and Nelson, 2003). As one CIO describes the current business transition (Reich and Nelson, 2003, p. 32):

> I think the whole e-business paradigm will radically change the way our customers will interact with us, the way we think about other businesses, what our core business is, as well as completely rip away any sense of consistency in terms of achieving infrastructure at a time when we haven't yet quite figured out how to integrate what we already have.

Managing complexity in enterprise architecting

Modeling is essential to describing and understanding enterprise architecting (EA). There are three reasons to model (Kaisler *et al.*, 2005):

(1) to visualize the EA, its evolution, and its generational impact on the existing architecture;

(2) to depict to stakeholders the control and data flow through the architecture; and

(3) to conduct end-to-end performance analyses.

Large organizations will have ongoing projects that remediate, renovate, or replace information systems, as well as develop new systems. The challenge is (Kaisler *et al.*, 2005):

- to coordinate schedules to ensure that interdependencies mesh;
- to ensure that intersystem constraints at the interfaces are resolved; and
- to ensure interoperability at the syntactic and semantic interactions between information systems.

Operational consistency must be preserved while the organization continues to evolve the architecture. Particularly in the context of Section 404 compliance, system changes cannot impact on day-to-day operations, so careful scheduling and integration of changes to the architecture is required.

The ability to model and align business operations and processes in ERP architecture is lacking (Kaisler *et al.*, 2005). While there are a number of tools such as Metis, Popkins SA, Troux, Orbus, and Casewise Corporate Modeler that are beginning to address these issues, a well-integrated solution was not available in 2004-2005. Most EAs are built on top of legacy systems and frequently require individual components of the EA to be remediated, renovated, replaced, or developed. Every modification to an EA introduces change to the underlying technical infrastructure, whether new hardware, software, or telecommunications platforms, or just parametric changes.

Themes are consistent in areas related to enterprise systems

Outsourcing of programming and services and network security can pose either primary or secondary risks to financial information. Consistent with Deloitte & Touche (1999), Deloitte Consulting (1999), Benesh (1999), Somers and Nelson (2001), and Reich and Nelson (2003), competencies in project management and related disciplines as applied to outsourcing and network security can affect SOX compliance. Common problems for outsourcing programming include (Kolawa, 2004):

- lapses in schedules;
- incomplete requirements; and
- coding quality that falls short of expectations.

Incomplete requirements and coding quality are potentially serious Section 404 compliance issues. Most outsourcing efforts of services fall midway between micromanagement of offshore processes and throwing processes "over the wall" (Tas and Sunder, 2004).

Closely related to project management, change management and ongoing assessment of changes made in the course of network security are key factors of success. Alberts, a senior member of the Networked Systems Survivability Program at the Software Engineering Institute at Carnegie Mellon, described the broader issue of security as being primarily perceived as a technology problem when in fact it is an organizational problem with a technology component (Zorz, 2003). Alberts and Dorofee (2002) authored a comprehensive framework to evaluate organizational and technological issues to understand and address IT security risks. The framework:

- balances information assets, business needs, threats, and vulnerabilities;
- measures against known or accepted good security practices; and
- establishes organization-wide strategy and risk mitigation plans.

After the initial implementation of SOX

A continued emphasis on change management

A project characterized by a one-time change agent, created for the first time implementation, may develop an initially doable, but unsustainable and potentially un-testable approach to Section 404 compliance (Kola, 2004). It concentrates responsibility for compliance in the hands of a few, and is often typified by retention of outside consultants who take the process knowledge with them when they leave companies. There are several approaches used to maintain the momentum to integrate Section 404 into operational practices, including the expanded use of the internal audit function, risk identification and management programs, integrated information systems to support Section 404 compliance; and active change management to design and implement Section 404 compliance as the business evolves (Dittmar, 2004).

Software to manage risks

Application-level controls and general computer controls have been major focuses of attention in year-one projects (Dittmar, 2004). Many companies have used technology to help manage their 404 efforts, and to provide control repositories and audit trails. The software solutions for SOX compliance include the creation of graphical representations, project planning, real-time monitoring, process integration, document creation, and long-term records management (Hamerman *et al.*, 2005). The primary functional characteristics of the software solution are organizational configuration, project planning, a control framework, process documentation, workflow, and document/content management. Executive compliance dashboard solutions should provide real-time, role-based views that provide appropriate levels of access to ongoing compliance activities. Many vendors have provided very sophisticated dashboards – SAS, IBM, and PeopleSoft – that provide real-time, role-based views into the compliance of the enterprise, synchronized through directory services. Technology enables the integration of financial and internal control monitoring and reporting, which will be key to most large and complex enterprises (Dittmar, 2004). In most cases, the efficiencies gained by leveraging such technology will rapidly offset the implementation costs.

SOX is a current driving force in the design of commercial database technologies (Hagan, 2004). Data type support for extensible markup language (XML), image, and text and geographic referencing and analysis, as well as user-defined enhancements,

are now the norm and will be required in data management systems. Complex data requirements, combined with SOX compliance, are yielding a rapid migration from unconsolidated file storage to consolidated database repositories that are secure, recoverable, and auditable.

Frameworks to support SOX compliance

In addition to COSO, several frameworks have been issued to provide guidelines and best practices and assist with the definition, assessment, reporting on and improvement of internal control in organizations (Colbert and Bowen, 1996; Salle and Rosenthal, 2005). These frameworks include COBIT, the Institute of Internal Auditors Research Foundation's Systems Electronic Security Assurance and Control (eSAC) and the IT Infrastructure Library (ITIL). Several published authors in the field describe COBIT as the generally accepted IT standard for governance (Ramos, 2004; Pathak, 2003).

COBIT categorizes IT processes into four domains (Table II). COBIT was originally released as an IT process and control framework linking IT to business requirements (IT Governance Institute, 2005). Beginning with the addition of *Management Guidelines* in 1998, COBIT is now being used more and more as framework for IT

Domain	Key processes
Planning and organization	Define a strategic plan
	Define the information architecture
	Define the IT organization and relationships
	Communicate management aims and direction
	Manage human resources
	Ensure compliance with external requirements
	Assess risks
	Manage quality
Acquisition and implementation	Acquire and maintain application software
	Acquire and maintain technology infrastructure
	Develop and maintain procedures
	Install and accredit systems
	Manage changes
Delivery and support	Define and manage service levels
	Manage third-party service levels
	Manage performance and capacity
	Ensure continuous service
	Ensure systems security
	Educate and train users
	Manage the configuration
	Manage problems and incidents
	Manage data
	Manage facilities
	Manage operations
Monitoring	Monitor the processes
	Assess internal control adequacy
	Obtain independent assurance

Table II.
COBIT IT processes

Source: Ramos (2004)

governance (Ramos, 2004). COBIT's overall goal of an entity's IT-related control structure is to ensure the delivery of the necessary information to the business. COBIT describes the goals for IT governance to include alignment of IT with the business and maximize the benefits to the entity, and requires the usage of IT resources responsibly (Ramos, 2004).

Little academic literature has been published that investigates the utilization of COBIT (Ridley *et al.*, 2004). COBIT and related sources are produced by the Information Systems Audit and Control Association (ISACA, 2005) and the IT Governance Institute (2005) and are not referred to by many academic authors. A handful of studies that benchmark the adoption or use of COBIT have been published by peer reviewed sources (Guldentops *et al.*, 2002; Fedorowicz, and Ulric, 1998; Tongren and Warigon, 1997). The IT Governance Institute does provide the investigator an excellent source of case studies on COBIT outcomes. Case studies from the IT Governance Institute, as well as personal contacts in companies that are currently following COBIT, are two primary sources available to assist in the evaluation of the implementation of COBIT in an IT organization.

IT governance and SOX: where we go from here

IT governance describes the selection and use of organizational processes to make decisions about how to obtain and deploy IT resources and competencies (Luftman *et al.*, 2004). IT governance is about who makes these decisions (power), why they make them (alignment), and how they make them (decision process). Symptoms of ineffective IT governance include low project success rates and the ineffective IT alignment with business objectives. Overall IT project success rates have only recently improved to 34 percent while "challenged projects" still remain at 51 percent (The Standish Group, 2003). Potential alignment issues in IT governance for SOX compliance are indicated by two recent surveys. A survey of top *Fortune* 100 companies conducted by Worthen (2003) reports that most executives viewed compliance with SOX as a finance issue and that it was premature for the CIO to be involved. A Gartner survey of 75 senior compliance executives found that 37 percent of companies have no IT representation on SOX compliance teams (Leskeia and Logan, 2003). A consistent theme throughout the recent history of enterprise systems development is the lack of systematic competencies in several related disciplines. Change management, project management, reporting procedures, process engineering, and prioritization of resources are among those skills that have been identified with underperforming ERP applications. Outsourcing of programming and services and enterprise architectural modeling requires effective execution of project management and related disciplines and is consistent with the themes cited by Deloitte & Touche (1999), Deloitte Consulting (1999), Benesh (1999), Somers and Nelson (2001) and Reich and Nelson (2003)

A linear extension of ERP history suggests that IT governance may be a roadblock in the adoption of SOX and COSO. Software and practice implementations to manage risk to comply with SOX require all of the ERP competencies described earlier plus the complete integration of SOX and COSO. As we move into the period following the first year of SOX compliance and as research identifies SOX compliance failures, we will begin to understand whether the same issues that plagued ERP systems continue unabated in a new environment. A significant incentive for SOX compliance is the

punitive measures for the CEO and CFO specified in SOX and may play a role in the success rates.

To best practice and competitive advantage

COSO describes internal control as a process that is affected by people (COSO, 2005; Damianides, 2005). The IT organization must be able to support the internal controls of the organization on a systematic and repeatable level – the controls are integral to the operation of the enterprise (Table III).

The Software Engineering Institute (SEI) at Carnegie Melon developed the original capability maturity model (CMM) and continues to evolve with new CMM products (Software Engineering Institute, 2005). The internal control reliability model parallels concepts in the SEI CMM (Table III) (SEC, 2005; Ramos, 2004). The underlining premise of the CMM is that if an organization does not have a defined and standardized software development process it is unable to provide a consistent and reliable product. That underlying premise also applies to processes to support SOX compliance. An IT organization with a consistent and reliable development process will contribute to the company's competitive and strategic advantage.

Several formal and informal frameworks exist to help move the IT organization to high levels of CMM maturity. Kola (2004) describes a process of moving to a practice approach before the adaptation of best practices. The practice approach formalizes and sets into motion:

- standard operating procedure;
- consistent behaviors; and
- routine monitoring.

The practice approach is repeatable and necessary for auditor testing. Best practices are characterized by:

- common structures for Sections 302, 404, 409, and 802;
- optimized management responsiveness; and
- defined business benefits such as reduced liabilities.

Creating value is:

- to create business processes that resolve Section 302, 404, 409, and 802 issues before they happen;
- to use the company's resources more effectively; and
- to establish the capability of the company to execute to a defined and standardized process (Cobb, 2004).

The best practice approach aligns the standards of adequacy for disclosure controls with those for internal controls and enables management to meet accelerated disclosure deadlines.

As described earlier, the COBIT framework provides "good practices" developed by a consensus of experts in the field and defines a process framework against a set of 34 high-level control objectives, one for each of the IT processes, grouped into four

Reliability level	Characteristics of reliability				
	Documentation	Awareness and understanding	Perceived value	Control procedures	Monitoring
Initial	Very limited	Basics awareness	Uniformed	Ad hoc, unlinked	
Informal	Sporadic, inconsistent	Understanding not communicated	Controls separate from business operations	Intuitive, repeatable	
Systematic	Comprehensive and consistent	Formal communication and some training	Controls integral to operations	Formal, standardized	
Integrated	Comprehensive and consistent	Comprehensive training	Control process part of strategy	Formal, standardized	Periodic monitoring beings
Optimized	Comprehensive and consistent	Comprehensive training on control related matters	Commitment to continuous improvement	Formal and standardized	Real-time monitoring

Source: Ramos (2004)

Table III.
Summary of internal control reliability model

domains (Table II). The IDEAL model authored by Gremba and Myers (2005) of SEI walks through five distinct phases of:

(1) laying the groundwork for a successful improvement effort;
(2) a diagnosis of where you are relative to where you want to be;
(3) planning the specifics of how you will reach your destination;
(4) executing the work to plan; and
(5) learning from the experience and improving the ability to adopt new technologies in the future.

Whether the CIO adopts COBIT, the IDEAL Model, or another framework for a long-term commitment, additional steps should be taken to ensure ongoing change management activities following the initial installation of SOX compliance (Dittmar, 2004; Cannon and Growe, 2004).

Conclusion

The ERP competencies cited by Deloitte & Touche (1999), Deloitte Consulting (1999), Benesh (1999), Somers and Nelson (2001), and Reich and Nelson (2003) are necessary to implement software and processes to support SOX, EA, outsourcing of programming or activities, enterprise security, and enterprise initiatives such as COBIT or the IDEAL model. Among all variables including technology, process, and personnel, Barry Boehm led the early discussion to demonstrate the dramatic differences that personnel and competencies have on performance (Boehm, 1981). Consistent with Boehm and ERP research cited in this paper, Xia and Lee (2004) identified the influence of organization and personnel in large IT projects. In their study of 541 large IT projects across several industries, organizational aspects, including the use of qualified personnel were the leading factor contributing to project success. CIOs should attend to organizational factors including the recruitment and retention of qualified personnel to establish competencies as a very high priority in the execution of SOX and subsequent compliance activities.

References

Alberts, C. and Dorofee, A. (2002), *Managing Information Security Risks: The OCTAVE Approach*, Addison-Wesley, New York, NY.

Benesh, M. (1999), "Managing your ERP project", *Software Testing and Quality Engineering*, July/August, pp. 38-43.

Boehm, B. (1981), *Software Engineering Economics*, Prentice-Hall, Upper Saddle River, NJ.

Cannon, D. and Growe, G. (2004), "SOA compliance: will IT sabotage your efforts?", Wiley Periodicals, Inc, published online in Wiley InterScience, available at: www.interscience.wiley.com

Chan, S. (2004), "Sarbanes-Oxley: the IT dimension", *The Internal Auditor*, Vol. 61 No. 1, pp. 31-3.

Chang, S., Gable, G., Smythe, E. and Timbrell, G. (2000), "A Delphi examination of public sector ERP implementation issues", *Proceedings of the Twenty First International Conference on Information Systems*, Information System Management Research Centre, Faculty of Information Technology, Queensland University of Technology, Brisbane, pp. 494-500.

CIO Insight/Gartner (2004), "EXP research: Sarbanes-Oxley 2004: are you ready to comply?", available at: www.cioinsight.com

Cobb, C.G. (2004), "Sarbanes-Oxley: pain or gain?", *Quality Progress*, Vol. 37 No. 11, pp. 48-52.

Colbert, J. and Bowen, P. (1996), "A comparison of internal controls: COBIT, SAC, COSO and SAS 55/78", *IS Audit & Control Journal*, Vol. 4, pp. 26-35.

COSO (2005), "FAQs, for COSO's enterprise risk management – integrated framework", available at: www.coso.org/Publications/ERM/erm_faq.htm

Damianides, M. (2005), "Sarbanes-Oxley and IT governance: new guidance and IT control and compliance", *Information Systems Management*, Winter.

Decker, S. and Lepeak, S. (2003), *Connecting to ERP for SOX 404 Assessments*, META Group, Stamford, CT, available at: www.metagroup.com

Deloitte & Touche (1999), "Maximizing the value of ERP enabled processes", *The Review*, 18 January.

Deloitte Consulting (1999), *ERP's Second Wave*, Deloitte Consulting, Atlanta, GA.

Dittmar, L. (2004), "What will you do in Sarbanes-Oxley's second year?", *Financial Executive*, Vol. 20 No. 8, pp. 17-18.

Fedorowicz, J. and Ulric, J. (1998), "Adoption and usage patterns of COBIT: results from a survey of COBIT purchasers", *Information Systems Audit & Control Journal*, Vol. 6, pp. 45-51.

Garretson, C. (2003), "Under the gun", *Network World*, Vol. 20 No. 35, p. 38.

Gremba, J. and Myers, G. (2005), "The IDEAL model: a practical guide for improvement", Carnegie Melon Software Engineering Institute, available at: www.sei.cmu.edu/ideal/ideal.bridge.html

Guldentops, E., Van Grembergen, W. and De Haes, S. (2002), "Control and governance maturity survey: establishing a reference benchmark and a self-assessment tool", *Information Systems Control Journal*, Vol. 6, pp. 32-5.

Hagan, S. (2004), "Plenary session: driving forces in database technology", *Proceedings of the 20th International Conference on Data Engineering (ICDE'04)*, IEEE, New York, NY.

Hamerman, P., Markham, R., Orlov, L. and Teubner, C. (2005), *Sarbanes-Oxley Solutions – Invest Now or Pay Later Hybrid Applications Emerge for Internal Controls Compliance*, Forrester Research, Cambridge, MA, available at: www.forrester.com

Hawking, P., Stein, A. and Foster, S. (2004), "Revisiting ERP systems: benefit realization", paper presented at the 37th Hawaii International Conference on System Sciences, ACM, available at: http://csdl.computer.org/

Heffes, E. (2005), "FEI CEO's 2005 top 10 financial reporting issues", *Financial Executive*, Vol. 21 No. 1, available at: www.fei.org

Information Systems Audit and Control Association (2005), "About ISACA", available at: www.isaca.org

IT Governance Institute (2005), "About ITGI", available at: www.itgi.org

Kaarst-Brown, M. and Kelly, S. (2005), "IT governance and Sarbanes-Oxley: the latest sales pitch or real challenges for the IT function?", *Proceedings of the 38th Hawaii International Conference on System Sciences – 2005*, IEEE, New York, NY.

Kaisler, S., Armour, F. and Valivullah, M. (2005), "Enterprise architecting: critical problems", *Proceedings of the 38th Hawaii International Conference on System Sciences*, IEEE, New York, NY.

Kola, V. (2004), "Sarbanes-Oxley section 404: from practice to best practice", *Financial Executive*, Vol. 20.

Kolawa, A. (2004), "Outsourcing: devising a game plan, what types of projects make good candidates for outsourcing", *Queue*, Vol. 2 No. 8, pp. 56-62.

Krasner, H. (2000), "Ensuring e-business success by learning from ERP failures", *IT Pro*, January-February.

Lepeak, S. (2004), *Sarbanes-Oxley: How Can I Ensure True Success?*, META Group Services, available at: www.metagroup.com

Leskeia, L. and Logan, D. (2003), "Sarbanes-Oxley Compliance Demands IS Involvement", Gartner, available at: www.gartner.com/

Louwers, T., Ramsey, R., Sinason, D. and Strawser, J. (2005), *Auditing and Assurance Services*, McGraw-Irwin, New York, NY.

Luftman, J., Bullen, C., Liao, D., Nash, E. and Neumann, C. (2004), *Managing the Information Technology Resource*, Pearson Prentice-Hall, Upper Saddle River, NJ.

Marlin, S. (2003), "Rules of the road", *InformationWeek*, No. 958, p. 40.

Mead, N.R. and Mcgraw, G. (2004), "Regulation and information security: can Y2K lessons help us?", *IEEE Security and Privacy*, IEEE, New York, NY.

Pathak, J. (2003), "Internal audit and e-commerce controls", *Internal Auditing*, Vol. 18 No. 2, pp. 30-4.

Proctor, P. (2004), "Sarbanes-Oxley security and risk controls: when is enough enough?", Stamford, CT, *Infusion: Security & Risk Strategies*, META Group, available at: www.metagroup.com

Public Company Accounting Oversight Board (PCAOB) (2005), "Center for enforcement tips, complaints and other information", available at: www.pcaobus.org/Enforcement/Tips/index.asp

Public Company Accounting Oversight Board (PCAOB) (2002), "Sarbanes-Oxley act of 2002", Public Law 107-204, 107th Congress, available at: www.pcaobus.org

Ramos, M. (2004), *How to Comply with Sarbanes-Oxley Section 404*, Wiley, Hoboken, NJ.

Reich, B.H. and Nelson, K. (2003), "In their own words: CIO visions about the future of in-house IT organizations", *The Database for Advances in Information Systems*, Vol. 34 No. 4.

Ridley, G., Young, J. and Carol, P. (2004), "COBIT and its utilization: a framework from the literature", *Proceedings of the 37th Hawaii International Conference on System Sciences – 2004*, IEEE, New York, NY.

Salle, M. and Rosenthal, S. (2005), "Formulating and implementing an HP IT program strategy using COBIT and HP ITSM", *Proceedings of the 38th Hawaii International Conference on System Sciences – 2005*, IEEE.

SAP (2005), Home page, available at: www.sap.com

SEC (2005), "Regulation S-K, §229.308, Item 308", available at: www.sec.gov/divisions/corpfin/forms/regsk.htm#internal

Software Engineering Institute (2005), "Capability maturity models", available at: www.sei.cmu.edu

Somers, T.M. and Nelson, K. (2001), "The impact of critical success factors across the stages of enterprise resource planning implementations", *Proceedings of the 34th Hawaii International Conference on System Sciences – 2001*, IEEE, New York, NY.

(The) Standish Group (2003), "Latest Standish group CHAOS report shows project success rates have improved by 50 percent", available at: www.standishgroup.com

Tas, J. and Sunder, S. (2004), "Financial services business process outsourcing", *Communications of the ACM*, Vol. 47 No. 5.

Tongren, J. and Warigon, S. (1997), "A preliminary survey of COBIT use EDP audit", *Control and Security Newsletter*, Vol. 25 No. 3, pp. 17-19.

Worthen, B. (2003), "Your risks and responsibilities; you may think the Sarbanes-Oxley legislation has nothing to do with you. You'd be wrong", *CIO*, Vol. 16 No. 15, p. 1.

Xia, W. and Lee, G. (2004), "Grasping the complexity of IS development", *Communications of the ACM*, Vol. 47 No. 5, pp. 68-74.

Ziff Davis (2004), "*CIO Insight Magazine* and Gartner EXP release major study on Sarbanes Oxley compliance", available at: www.ziffdavis.com

Zorz, M. (2003), "Interview with Christopher Alberts, a senior member of the technical staff in the Networked Systems Survivability Program at the Software Engineering Institute", available at: www.net-security.org (accessed 12 March).