Sarbanes–Oxley and Enterprise Security: IT Governance — What It Takes to Get the Job Done

William Brown and Frank Nasuti

Several sections of the Sarbanes–Oxley Act of 2002 (SOX) directly affect the governance of the information technology (IT) organization, including potential SOX certification by the chief information officer, Section 404 internal control assessments, "rapid and current" disclosures to the public of material changes, and authentic and immutable record retention. The Securities and Exchange Commission (SEC) requires publicly traded companies to comply with the Treadway Commission's Committee of Sponsoring Organizations (COSO) that defines enterprise risk and places security as a critical variable in enterprise risk assessment. Effective IT and security governance are examined in terms of SOX compliance. Motorola IT security governance demonstrates effective structures, processes, and communications; centralized security leaders participate with Motorola's Management Board to create an enabling security organization to sustain long-term change.

INTRODUCTION

In response to the series of business failures and corporate scandals that began with

WILLIAM C. BROWN, Ph.D., CPA, is an assistant professor at Minnesota State University–Mankato, College of Business. His professional experience includes teaching management information systems at both the undergraduate and graduate levels and serving for more than 25 years as a financial officer. He served as a chief financial officer in three companies that were Securities and Exchange Commission registrants. His education includes an MBA, a CPA, an MS in software engineering, and a Ph.D. in management information systems.

FRANK NASUTI, Ph.D., CPA, CICA, CFE, has served as a visiting and adjunct professor at Nova Southeastern University, Widener University, Temple University, and Rutgers University, teaching research methods, computer science, and accounting at both the doctoral and master's levels. His professional experience includes law enforcement as a special agent/criminal investigator, IT audit manager for a Big 4 accounting firm, internal audit director for a financial services company, and senior managing director for a major consulting firm. He founded The Institute for Internal Controls, a professional certification and research organization. His education includes a BS in accounting, an MBA in management, an MS in information science, and a Ph.D. in information systems. He is a CPA and holds the designations of certified internal controls auditor and certified fraud examiner.

Enron in 2001, the U.S. Congress enacted the Sarbanes–Oxley Act of 2002. The stated purpose of SOX (2002) is to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws. SOX outlines the duties of the chief executive officer (CEO), the chief financial officer (CFO), and the auditor, including making each personally responsible for ensuring the credibility of the financial reporting provided to stakeholders. Eleven sections of SOX (2002) define auditor and corporate responsibilities, including expectations for financial disclosures, strong penalties for white-collar crimes, and protection for "whistleblowers." Other regulatory measures, including the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Gramm–Leach–Bliley Act of 1999 (GLBA), the Fair Credit Reporting Act (FCRA), the Notification of Risk to Personal Data Act (NORPDA), and the Personal Information Protection and Electronic Documents Act (PIPEDA), may create financial and operational liabilities for the enterprise. The steps recommended in security governance may help align the enterprise to meet these specific regulatory measures but are not specifically addressed in this article.

The SEC offers little specific guidance on IT security, leaving the door open to interpretation as to the scope and nature of security initiatives for SOX compliance. The National Cyber Security Task Force recommended that the SEC define specific security requirements in future regulatory guidance. Although the SEC has not defined security requirements per se, the SEC is a very effective change agent and will assert itself if additional compliance measures are required (Mead & McGraw, 2004).

In connection with SOX compliance, the SEC does require the implementation of *Enterprise Risk Management – Integrated Framework* (ERM) authored by the Treadway Commission's Committee of Sponsoring Organizations (COSO). The ERM framework divides IT controls into two types (Ramos, 2004): (a) *general computer controls* and (b) *application-specific controls,* which will be described in more detail later in this article. The purpose of this article is to examine effective security governance for SOX in the IT organization. Christopher 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). COSO described internal control as a *process that is affected by people* (COSO, 2005; Damianides, 2005). Organizational design, behavior, and IT governance play very significant roles in whether the enterprise can successfully implement the ERM framework as defined by the Treadway Commission.

IT governance describes the selection and use of organizational processes to make decisions about how to obtain and deploy IT resources and competencies (Luftman, Bullen, Liao, Nash, & Neumann, 2004). IT governance is about who makes these decisions (power), why they make them (alignment), and how they make them (decision process). Forrester Research (Symons, 2005) offers a similar definition for IT governance: how decisions are made, who makes the decisions, who is held accountable, and how the results of decisions are measured and monitored. Specific to security governance for the IT organization, the National Cyber Security Task Force (2005) describes people, process, and technology as the key elements of IT security governance. The integration of people, processes, and technology requires the following:

- ☐ CEO participation in accountability, authority, and oversight of compliance
- ☐ Executive management of security commensurate with risk and integration policies within the operations
- ☐ Senior managers involved with risk assessment and the implementation of security policies and operations security

- ☐ A security program that integrates frameworks, methods, policies, procedures, technology, and business continuity plans
- ☐ Ongoing reporting to the management and Board of Directors

Control Objectives for Information and Related Technology (COBIT), a generally accepted framework for IT auditors that maps to SOX requirements (Chan, 2004; Ramos, 2004), categorizes IT processes into four domains. COBIT originally was released as an IT process and control framework linking IT to business requirements (IT Governance Institute, 2005a). Beginning with the addition of *Management Guidelines* in 1998, COBIT is now being used increasingly as a framework for IT governance (Ramos, 2004). Recent research suggests that certain characteristics of IT governance contribute to more effective alignment and execution of IT programs, including security governance (Weill & Ross, 2004). That research will be explored to complete the COBIT governance framework and to describe effective security governance to meet SOX compliance.

RECENT SECURITY SURVEYS AND SOX

Two recent surveys (CERT® Coordination Center, 2005; Computer Crime Research Center, 2005) suggest that security practitioners may have difficulty complying with SOX and other security frameworks. The 2004 CSI/FBI Computer Crime Survey reported that 20 percent of the 494 respondents representing a cross-section of industries said that they do not use IT security audits as a tool to assess their organizations' security vulnerabilities (Computer Crime Research Center, 2005). In the same survey, the percentage of respondents who experienced unauthorized use of computer systems in 2004 declined to 53 percent from 58 percent a year previously. Although this represented a significant improvement, it is still evident of an alarmingly high rate of unauthorized use. Four years earlier, the rate of unauthorized use reached a peak of 70 percent of survey respondents in the 2000 CSI/FBI Computer Crime and Security Survey and has declined in each consecutive year (Computer Crime Research Center, 2005). According to the survey results, 2004 financial losses resulted from, in descending order, virus attacks, denial of service, and theft of proprietary information, which cost the companies of the respondents $55.0 million, $26.0 million, and $11.4 million, respectively. The 2004 CSI/FBI Computer Crime and Security Survey also reported an increasing reluctance by companies to belong to information-sharing organizations. Over 50 percent of the survey respondents cited the perception that negative publicity would hurt their company's stock or image. The survey respondents in the financial, utility, and telecommunications sectors reported that SOX is having an impact on the organization's security. With the full implementation of SOX, it may be more difficult to assess the scope of computer crimes as companies comply with SOX and become more reluctant to share information. However, the survey revealed that security practitioners understand that security breaches have very serious consequences.

A second survey, the 2004 E-Crime Watch Survey conducted by the U.S. Secret Service and Carnegie Mellon University Software Engineering Institute, reported an increase in E-crimes as well as network, system, and data intrusions (CERT® Coordination Center, 2005). Leading causes of security breaches reported in this survey were similar to those reported in the 2004 CSI/FBI Computer Crime and Security (Computer Crime Research Center, 2005). Respondents reported the following security breaches: viruses (77 percent of respondents), denial of service (44 percent), generation of SPAM or junk e-mail (38 percent), unauthorized access by an *insider* (36 percent), phishing or sending fraudulent e-mails seeking secure information (31 percent), and unauthorized access by an outsider (27 percent). Significant to SOX compliance, 7 percent of the respondents

reported critical system disruption affecting customers and loss of current or future revenue from insider intrusion. Also significant to SOX and potentially material to financial statements (depending on the size of the company), 3 percent of the respondents reported monetary losses that exceeded $10.0 million in connection with security breaches.

Lack of protection from once-proven technologies, new threats, and an onslaught of new legislation have changed the perspective of corporate management and Board of Directors toward IT security and governance. Concurrent with the high profile prosecution of Enron and WorldCom officers, the 2004 E-Crime Watch survey (CERT® Coordination Center, 2005) reaffirmed that current employees remain a very serious security threat. Threats ranging from terrorist attacks to phishing continue to demonstrate the need for robust security governance. Regulatory measures including HIPAA, GLBA, FCRA, NORPDA, and PIPEDA and the legal liabilities associated with those laws have led to the boardroom realization that security is no longer just an IT issue. Effective IT and security governance is essential for SOX compliance and ERM.

SARBANES–OXLEY AND IT GOVERNANCE

Key sections of SOX compliance that directly involve IT include Sections 302, 404, 409, and 802 (SOX, 2002).

- ☐ Section 302 requires corporate officers 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.

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

Section 302

While the CEO and the Board of Directors are accountable for overall corporate management, SOX also impacts IT administration, including organization governance, the responsibilities of chief information officers (CIOs), budgets, vendors, outsourcers, and business continuity plans. CEOs and CFOs may require their IT organizations to provide proof that automated portions of financial processes have appropriate controls, that computer-generated financial reports are accurate and complete, and that any exceptions are captured and reported in a timely manner (Kaarst-Brown & Kelly, 2005).

Recent surveys of CIOs reported that 44 percent of the companies required the CIO to certify financial results under SOX compliance (CIO Insight/Gartner, 2004). Gartner and various CIO journals have suggested the SEC eventually may 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 information and certification from those individuals who are directly responsible. 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 or operating effectiveness of internal controls.

Whether the reported 44 percent (CIO Insight/Gartner, 2004) will increase or decrease over time remains to be seen. In-depth interviews with over 50 CIOs in the United States and Canada showed that rapid strategic business change and E-business and technology complexity will be significant drivers in the near future (Reich & 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 (2005), is driving pervasive change in the internal controls of the enterprise. Section 404 requires the management of a public company and for the company's independent auditor to issue two new reports at the end of every fiscal year (SOX, 2002). These reports must be included in the company's annual report filed with the SEC. Under Section 404, management also must 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 (SOX, 2002). These management statements are not enough, however; the company's auditor also must attest to the truthfulness of these management internal control assertions.

COSO (2005) of the Treadway Commission recommended the ERM integrated framework to manage and reduce risks, to be applicable to all industries, and to encompass all types of risk. Moreover, the ERM framework recognizes that an effective ERM 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, Ramsey, Sinason, & Strawser, 2005).

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

1. "Tone at the top" that positively influences the attitude of the personnel
2. Identification of risks, objectives, and the methods to manage the risks
3. Activities and procedures that are established and executed to address risks
4. Information systems to capture and exchange the information needed to conduct, manage, and control its operations
5. The monitoring of and responses to changing conditions as warranted

COSO created a framework that divides IT controls into two types (Ramos, 2004): (a) general computer controls and (b) application-specific controls. General controls include the following:

- ☐ Data center operations (e.g., job scheduling, backup and recovery)
- ☐ Systems software controls (e.g., acquisition and implementation of systems)
- ☐ Access security
- ☐ Application system development and maintenance controls

Application controls are designed to perform the following:

- ☐ Control data processing
- ☐ Ensure the integrity of transactions, authorization, and validity
- ☐ Encompass how different applications interface and exchange data

The ERM framework, a cornerstone of Section 404 and COSO, requires ongoing feedback from throughout the company. This feedback information must be current, accurate, and sufficiently robust to support the analysis of different risk responses (COSO, 2005). Many firms are implementing risk management applications to assist with internal control and assessment processes (Decker & Lepeak, 2003).

A main objective of these tools is to lower external audit verification costs.

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 (SOX, 2002). For example, a Section 409 compliance consideration for IT would be a situation where a computer virus knocked out the supply chain and materially affected the financial performance on a quarterly financial report (Proctor, 2004). This would be a disclosable 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 (2002) has a direct impact on data management, data and system security, and business recovery practices. The CIO must understand the requirements and ensure that the appropriate policies are in place, including ongoing compliance.

GOVERNANCE AND THE MATURITY MODEL

The IT Governance Institute (2005a, 2005b) issued a governance model that provides the structure and practices for four IT domains:

1. Plan and organize the strategic plan, architecture, IT organization, human resources, and compliance with external requirements (including SOX); assess risks; manage projects; and manage quality.
2. Acquire and implement software, hardware, infrastructure, and procedures; install and accredit systems; and manage changes.
3. Deliver and support service, performance and capacity, systems security, and user training; assist and advise customers; and manage problems and incidents, data, facilities, and operations.
4. Monitor processes, assess internal controls, obtain independent assurance, and provide for the independent audit.

The organizational design challenge is to ensure that the four domains of IT governance can sustain the necessary activities to meet SOX compliance.

A useful assessment is to compare the four domains of IT governance with the internal control reliability model. Internal controls or Section 404 compliance is a major provision of SOX. The internal control reliability model maps documentation, awareness and understanding, perceived value, control procedures, and monitoring of internal controls to five levels of maturity (Ramos, 2004). At the *systematic level* of the internal control reliability model, documentation is comprehensive, controls are integral to operations, and control procedures are formal and consistent, but compliance is not being monitored (see Table 1). Compliance with Section 404 is attained when the four domains of IT governance are aligned with the internal controls maturity model. The underlying premise of the internal controls maturity model (see Table 1) is that if an organization does not have defined and standardized processes, it is unable to provide consistent and reliable services. Standardized processes to provide consistent and reliable IT services are critical to SOX compliance. Maturity in all four domains of the IT governance model is required to sustain SOX compliance.

The IT Governance Institute (2005a, 2005b) and Forrester Research (Symons, 2005) have described the maturity levels of IT governance. Mapping the maturity levels of an organization to the internal control reliability model can provide some insight into whether a particular IT organization can meet SOX compliance. The four levels of Forrester Research's IT governance maturity are (a) ad hoc, (b) fragmented, (c) consistent, and (d) best practices (Symons, 2005). An *ad hoc* IT organization in maturity produces an *initial* level of reliability in internal controls and would be unacceptable

TABLE 1 Internal Control Reliability Model

Reliability Level	Characteristics of Reliability: Documentation	Awareness and Understanding	Perceived Value	Control Procedures	Monitoring
Initial	Very limited	Basic awareness	Unformed	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 begins
Optimized	Comprehensive and consistent	Comprehensive training on control-related matters	Commitment to continuous improvement	Formal and standardized	Real-time monitoring

Adapted from *How to Comply with Sarbanes–Oxley Section 404: Assessing the Effectiveness of Internal Control*, by Michael Ramos, John Wiley & Sons, Hoboken, NJ, 2004.

for SOX compliance. In contrast, an organization at the *best practice* maturity level has been using best practices for a period of time and has an optimized IT portfolio. A best practice maturity level would meet SOX compliance. The IT organization must evolve though internal development to integrate best practices into its IT governance model.

Before a best practice is adopted and integrated into the governance model, a practice approach should be developed and implemented (Kola, 2004). The practice approach formalizes and sets into motion (a) a standard operating procedure, (b) consistent behaviors, and (c) routine monitoring. The practice approach is repeatable and necessary for auditor testing. Best practices are characterized by (a) common structures for Sections 302, 404, 409, and 802; (b) optimized management responsiveness; and (c) defined business benefits such as reduced liabilities. Creating value is (a) creating business processes that resolve Section 302, 404, 409, and 802 issues before they happen; (b) using the company's resources more effectively; and (c) establishing 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.

Several formal and informal frameworks, including COBIT, ISO 17799, and IT Infrastructure Library (ITIL), which are explained in the following section, can help move the IT organization to high levels of maturity. Each framework offers particular features that can contribute to the overall security governance framework adopted by the enterprise. Security governance for an enterprise should include some part of each framework to build a comprehensive IT security governance strategy.

COBIT, ITIL, AND ISO 17799 FRAMEWORKS

COBIT is a generally accepted framework that maps well to SOX requirements (Chan, 2004; Ramos, 2004). COBIT and related sources are produced by the Information Systems Audit and Control Association (ISACA, 2005) and the IT Governance Institute (2005b). The COBIT framework provides "good practices" developed by a consensus of experts in the field and defines a process framework against a set of high-level control objectives, one for each of the IT processes, grouped into four domains (see Table 2).

According to the "Board Briefing on IT Governance" (IT Governance Institute,

TABLE 2 COBIT IT Processes

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

Adapted from *How to Comply with Sarbanes–Oxley Section 404: Assessing the Effectiveness of Internal Control*, by Michael Ramos, John Wiley & Sons, Hoboken, NJ, 2004.

2005a), the overall objectives of IT governance activities are (a) to understand the issues and strategic importance of IT, (b) to ensure that the enterprise can sustain its operations, and (c) to ascertain that it can implement the strategies required to extend its activities into the future. The IT Governance Institute (2005a) has provided an extensive compilation of leadership, value creation, performance management, governance frameworks, governance officers, and enterprise architecture implementation. The IT Governance Institute integrates numerous recognized best practices, frameworks, and processes, including the balanced scorecard, "Board Briefing on IT Governance," Capability Maturity Model, COSO ERM Integrated Framework, European Framework for Quality Management, Enterprise Architecture, ISO 9001–2000, Malcolm Baldridge Quality Criteria Framework, OECD Principles of Corporate Governance, and the Technical Reference Model.

ISO 17799 is a detailed "what to do" security standard that is organized into 10 major sections, each covering a different topic or area ("What is: ISO 17799," 2001): (a) business continuity planning, (b) system access control, (c) system development and maintenance, (d) physical and environmental security, (e) compliance, (f) personnel security, (g) security organization, (h) computer and network management, (i) asset classification and control, and (j) security policy. ISO 17799 has a narrow focus on security management and cannot stand alone as a security governance standard (Stolovitch, 2004; Symons, 2005). ISO 17799 can play a meaningful role in risk management assessment and therefore a role in security governance.

ITIL, initially developed in the U.K. by the Office of Government Commerce,

defines a broad range of processes that are considered best practices and are documented in a series of books. Processes include (a) incident management, (b) change management, (c) problem management, (d) service-level management, (e) continuity management (disaster recovery), (f) configuration management, (g) release management, (h) capacity management, (i) financial management, (j) availability management, (k) security management, and (l) help desk management. ITIL is extremely useful in improving the infrastructure to provide ongoing services through service management. ITIL should be applied as a tool within the context of a broader organizational strategy but should not be considered a comprehensive solution (Meyer, 2005).

The ITIL security management framework examines security from the service provider perspective, identifying the relationship between security management and the IT security officer as well as outlining how it provides the level of security necessary for the entire organization. COBIT and ITIL are complementary; COBIT takes on the role of audit and control, and ITIL takes on the role of best practices for services (Symons, 2005).

TRENDS IN SECURITY AND BUSINESS CONTINUITY PLANNING

Central information security groups are assuming greater seniority, with 40 percent or more of the security groups reporting directly to the CIO (Corporate Executive Board, 2003b). The central security is assuming responsibility for governing and coordinating policy and standards formulation, architecture, vendor selection, compliance auditing, vulnerability assessment, and intelligence gathering. Three emerging roles for the central information security organization are (a) awareness campaigns, (b) central password management, and (c) supply-chain security programs. Consistent with the research by Weill and Ross (2004), a direct reporting relationship by a centralized security organization creates the opportunity for more effective security governance through more collaborative opportunities between the business professionals and IT security management and through defined decision rights that involve technical decisions.

The 10 barriers to security and business continuity planning defined by the Corporate Executive Board Working Council (2003a) include (a) subjective risk prioritization, (b) poor risk communication, (c) security requirements mismatch, (d) siloed business protection, (e) unclear business continuity ownership, (f) insufficient user awareness, (g) inconsistent password policies, (h) incomplete business continuity preparedness, (i) poor crisis communication, and (j) external partner vulnerabilities. SOX requires compliance with the Treadway Commission's COSO ERM framework and therefore requires security risk prioritization and communication to be consistent with those standards. SOX (2002) Sections 302, 404, 409, and 802 are affected by all of these items, with the exception of subjective risk prioritization and poor risk communication.

RECENT RESEARCH IDENTIFYING EFFECTIVE IT AND SECURITY GOVERNANCE

In a survey of 256 IT organizations, the best predictor of effective IT governance performance was the percentage of managers in leadership positions who could accurately describe their IT governance processes (Weill & Ross, 2004). In above-average governance-performing enterprises, 45 percent or more of managers could describe accurately their IT governance, whereas in below-average performing enterprises, only a few managers in leadership positions could describe their governance process. Other factors associated with effective IT governance include (a) a higher percentage of senior managers who engage more often and more effectively in IT governance (committees, announcements, etc.), (b) more direct involvement of the senior business leaders in IT governance, (c) clearer business objectives for IT applications, (d)

more differentiated business strategies, (e) fewer approved exceptions, and (f) fewer changes in governance from year to year (Weill & Ross, 2004).

Of the 256 companies in Weill and Ross' (2004) survey, in those organizations with the *most effective* IT governance decisions, decisions were led by management, business unit leaders, and IT specialists in each of the respective areas:

- ☐ *IT principles* (clarification of the business role of IT): IT and top management or business unit leaders
- ☐ *IT architecture* (integration and standardization of IT requirements): IT specialists
- ☐ *IT infrastructure* (sharing and enabling of IT services): IT specialists
- ☐ *Business application need* (evaluation of business needs for purchased or developed applications): corporate and business units, with or without IT
- ☐ *IT investment* (funding for IT initiatives): IT and top management or business unit leaders

For those organizations with the *least effective* IT governance decisions, decisions were led by management, business unit leaders, and IT specialists in each of the respective areas:

- ☐ *IT principles*: top management or business unit leaders
- ☐ *IT architecture*: top management or business unit leaders
- ☐ *IT infrastructure*: top management or business unit leaders
- ☐ *Business application need*: corporate and business units, with or without IT
- ☐ *IT investment*: top management or business unit leaders

Perhaps it is no coincidence that a Gartner survey of 75 senior compliance executives found that 37 percent of companies had no IT representation on SOX compliance teams (Leskeia & Logan, 2003).

Weill and Ross (2004) reported that the *most effective* decision-making structures are

- ☐ Executive management committees
- ☐ IT leadership committees
- ☐ Business/IT relationship managers

The *least effective* IT decision-making structures are

- ☐ Capital approval committees
- ☐ Architectural committees

The most effective alignment processes are tracking IT projects and resources consumed. The least effective are charge-back mechanisms and tracking the business value of IT investments.

The methods of engagement include (a) senior management announcements that reinforce and alert governance changes; (b) formal committees to add weight and cross-functional influence; (c) a recognized advocate, owner, and organizational home; (d) a dialogue to educate and address concerns; and (d) a single place for governance information such as an intranet (Weill & Ross, 2004).

SECURITY GOVERNANCE AT MOTOROLA

Many enterprises are concerned with security, but Motorola has made it a strategic priority (Weill & Ross, 2004). Security governance secures the support of executive management through a Management Board for IT Principles and IT Investment, but the security leaders maintain the final decision authority over the security architecture and infrastructure. The decision-making process at Motorola security includes the following:

- ☐ *IT principles*: Management Board and security leaders
- ☐ *IT architecture*: security leaders
- ☐ *IT infrastructure*: security leaders
- ☐ *Business application need*: business leaders
- ☐ *IT investment*: Management Board and security leaders

Motorola's Corporate Information Security Officer participates at quarterly Management Board meetings with the following:

- ☐ An identification of Motorola's security risks and the alternatives for addressing them
- ☐ An education about the likelihood of various security breaches and the potential impacts of each threat
- ☐ Recommended security principles and priorities in certain areas of the business
- ☐ A budget that is approved separately from the rest of the IT budget.

Using a monarchy decision-making style, Motorola's Corporate Information Security Officer

- ☐ Implements security plans at both a corporate and business unit level
- ☐ Designs and builds appropriate technology with his support staff
- ☐ Works with IT architects at both the corporate and the sector levels to ensure that security measures are built seamlessly into the IT infrastructure and applications

As an example of how Motorola security integrates itself into the IT architecture and infrastructure, Motorola created a single, global department tasked with centrally rolling out standard configurations across the enterprise (Microsoft Executive Circle, 2004). Motorola's security organization is ultimately responsible for 65,000 desktop and portable computers plus embedded devices and other computers spread across the Americas, Europe, Africa, and Asia. Before centralizing the upgrades, updates using third-party software programs or complete security updates to protect Motorola's enterprise from viruses, hackers, and other security threats would take weeks. The company consolidated 600 domains into a single environment with nine child domains. Software updates that formerly took months are now completed in less than a week.

As another example of how Motorola security integrates itself into the IT architecture and infrastructure, Motorola developed the Extended Enterprise Protection Plan to evaluate risks in the supply chain, provide incentives for suppliers to improve their security, and identify areas where Motorola should take action internally to mitigate risks (Corporate Executive Board, 2003a). The plan includes six steps: (a) the identification of mission-critical partners, (b) a partner self-assessment using an ISO 17799 checklist, (c) a partner perimeter scan by a trusted third party to scan partner networks for vulnerabilities, (d) an offer of discounts to partners to access Motorola's vendors, (e) offers of cyber-insurance discounts, and (f) internal steps to mitigate any weakness that partners fail to address.

In the development of centralized security protection for 65,000 desktop and portable computers and supply chain security programs, Motorola's security governance identified and prioritized risks, communicated the risks to the business units and external partners, matched the security requirements to the needs, avoided siloed business protection, and managed external partner vulnerabilities. Motorola completed the business protection life cycle through three major security processes: (a) risk assessment, (b) policy setting and oversight, and (c) effective execution.

A strategic approach to information security transforms the IT security function from a set of ad hoc activities with an emphasis on technology to a coordinated approach of principles, behaviors, and adaptive solutions that map to business requirements (Proctor, 2004). A centralized security governance within Motorola works closely with a Management Board to define policies and priorities, to educate stakeholders, and to set budgets apart from IT operations. Motorola security leaders take sole possession and leadership of the IT security architecture and infrastructure. Motorola security has transformed itself from a loosely distributed set of domains across the world into a centrally coordinated approach to secure

65,000 computers and to administer a supply-chain security program. Effective decision-making structures, alignment processes, and methods of engagement are integral to effective security governance and ultimately to SOX compliance. Therefore, senior security leadership in governance structures such as Motorola likely can fully explain their governance process. Additionally, Motorola is likely to implement successfully a SOX compliance program that can change and evolve as the security environment changes and evolves.

The security governance framework includes (a) structures, (b) processes, and (c) communications (Symons, 2005). The Motorola governance framework includes (a) security managers within the security organization who report to the Management Board, (b) processes that include the management of security-related architecture and infrastructure for the enterprise, and (c) communications that directly involve the Management Board and include ongoing education and budget direction. Executive management committees (such as the Management Board at Motorola), IT leadership committees, and business/IT relationship managers are among the most effective governance structures for the IT organization and are likely to have a positive influence on security governance. The governance framework at Motorola has created an *enabling organization* rather than a *support organization*.

TO SUSTAINABLE CHANGE

A project characterized by a one-time change agent, created for first-time implementation, may develop an unsustainable and potentially untestable approach to Section 404 compliance (Kola, 2004). Such a short-term project 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. Most change initiatives, including the installation of new technology, downsizing, restructuring, or trying to change corporate culture, have had success rates of approximately 30 percent (Beer & Nohria, 2000). Management that emphasizes change from the top down to yield quick results often uses outside consulting firms. In contrast to a quick-change environment initiated by an outside consulting firm, ongoing change must be sustained by an organization in which employees are emotionally committed to solving the new challenges that continually arise. The most successful long-term approach is to integrate both a top–down and a bottom–up approach to change management. A successful integration of a top–down and bottom–up approach emphasizes several dimensions of change:

- ☐ Leadership both sets direction from the top and engages the staff below.
- ☐ Focus is simultaneously on the hard (structures and systems for SOX compliance) and on the soft (corporate culture to sustain ongoing responsiveness).
- ☐ Process involves planning for spontaneity.
- ☐ Reward system uses incentives to reinforce change but not to drive it.
- ☐ Consultants use expert resources who empower employees.

Several specific approaches can be used to maintain the momentum to integrate Section 404 into operational practices, including 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). Application-level controls and general computer controls have been major focuses of attention in first-year projects. Many companies have used technology to help manage their Section 404 efforts and to provide control repositories and audit trails.

CONCLUSION

In organizations with the *least effective* IT governance, decisions were led by management and business unit leaders in IT

principles, IT architecture, IT infrastructure, business application need, and IT investment. In organizations with the *most effective* IT governance, IT decisions were shared by management, business unit leaders, and IT specialists, with IT specialists leading the decision making in IT architecture and IT infrastructure. Motorola security governance demonstrates the role of effective structures, processes, and communications and how centralized security leaders participate with the Management Board. At Motorola, security specialists led the decision making for the IT architecture and IT infrastructure. The security governance framework must integrate the (a) structures, (b) processes, and (c) communications to create an *enabling* security organization for the security life cycle of (a) risk assessment, (b) policy setting and oversight, and (c) execution. The one-time consulting engagement by an outside consulting firm must be replaced by change management strategy that sustains long-term change.

References

Beer, M., & Nohria, N. (2000, May–June). Cracking the code of change. *Harvard Business Review, HBR OnPoint*.

Chan, S. (2004). Sarbanes–Oxley: The IT dimension. *The Internal Auditor*, *61*(1), 31–33.

CERT® Coordination Center. (2005). *2004 E-Crime Watch Survey shows significant increase in electronic crimes.* Available at http://www.cert.org/about/ecrime.html

CIO Insight/Gartner. (2004, May). EXP Research: Sarbanes–Oxley 2004: Are you ready to comply? Available at http://www.cioinsight.com

Cobb, C. G. (2004, November). Sarbanes–Oxley: Pain or gain? *Quality Progress, 37*(11), 48–52.

Committee of Sponsoring Organizations. (2005). *FAQs for COSO's Enterprise Risk Management—Integrated Framework.* Available at http://www.coso.org/Publications/ERM/erm_faq.htm

Computer Crime Research Center. (2005). *2004 CSI/FBI Computer Crime and Security Survey.* Available at http://www. crime-research.org/news/11.06.2004/423/

Corporate Executive Board. (2003a). *Securing extended enterprise partners*. Motorola, Inc., Working Council Research. Available at http://www.cio.executiveboard.com/

Corporate Executive Board. (2003b). *Trends in information security and business continuity planning from infrastructure protection to business enablement.* Available at http://www.cio.executiveboard.com/

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

Decker, S., & Lepeak, S. (2003). Connecting to ERP for SOX 404 Assessments. Available at the META Group Web site: http:// www.metagroup.com

Dittmar, L. (2004, November). What will you do in Sarbanes– Oxley's second year?" *Financial Executive*, *20*(8), 17–18.

Heffes, E. (2005, January–February). FEI CEO's 2005 top 10 financial reporting issues. *Financial Executive*, *21*(1). Available at http://www.fei.org

Information Systems Audit and Control Association. (2005). *About ISACA*. Available at http://www.isaca.org

IT Governance Institute. (2005a). *Board briefing on IT governance*. Available at http://www.itgi.org/

IT Governance Institute. (2005b). *Governance of the extended enterprise, bridging business and IT strategies.* Hoboken, NJ: John Wiley & Sons.

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

Kola, V. (2004, January–February). Sarbanes–Oxley Section 404: From practice to best practice. *Financial Executive*, *20*.

Leskeia, L., & Logan, D. (2003). *Sarbanes–Oxley compliance demands IS involvement.* Available at the Gartner, Inc., Web site: http://www.gartner.com/

Louwers, T., Ramsey, R., Sinason, D., & Strawser, J. (2005). *Auditing and assurance services.* New York: McGraw-Irwin.

Luftman, J., Bullen, C., Liao, D., Nash, E., & Neumann, C. (2004). *Managing the information technology resource.* Upper Saddle River, NJ: Pearson Prentice Hall.

Microsoft Executive Circle. (2004). *Motorola case study.* Available at the Microsoft Corporation Web site: http://www.microsoft. com

Mead, N. R., & McGraw, G. (2004). Regulation and information security: Can Y2K lessons help us? In *IEEE Security and Privacy,* IEEE.

Meyer, D. (2005). *Beneath the buzz: ITIL is a powerful tool, but holds pitfalls in store for those who get obsessed with it.* Available at the CIO.com Web site: http://www.cio.com/leadership/buzz/column.html?ID=4186

National Cyber Security Partnership. (2005). *Governance.* Available at http://www.cyberpartnership.org/init-governance.html

Proctor, P. (2004). Sarbanes–Oxley security and risk controls: When is enough enough? In *Infusion: Security & Risk Strategies.* Available at the META Group Web site: http://www.metagroup.com

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

Ramos, M. (2004). *How to comply with Sarbanes–Oxley Section 404.* Hoboken, NJ: John Wiley & Sons.

Reich, B. H., & Nelson, K. (2003). In their own words: CIO visions about the future of in-house IT organizations. *The Database for Advances in Information Systems, 34*(4).

Sarbanes–Oxley Act of 2002, Public Law 107–204 (2002). Available at http://www.pcaobus.org

Stolovitch, D. A. (2004, January 30). *Canadian ISO 17799 User Conference, Sun Life's experience with security governance and ISO 17799*. Available at http://www.scienton.com/7799ug/ Papers.html

Symons, C. (2005, March 29). *IT governance framework, structure, processes, and communication.* Available at the Forrester Research Web site: http://www.forrester.com/

Weill, P., & Ross, J. (2004). *IT governance: How top performers manage IT decision rights for superior results*. Boston: Harvard Business School Press.

What is: ISO 17799? (2001). Available at the Risk Associates Web site: http://www.securityauditor.net/ISO17799/what.htm

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