IT Security and Sarbanes-Oxley Compliance:

Conference Summary of Findings and Conclusions

August 2005

CYBER SECURITY INDUSTRY ALLIANCE REPORT
IT Security and Sarbanes-Oxley Compliance: Conference Summary of Findings and Conclusions

I. Introduction

Section 404 of the Sarbanes-Oxley Act of 2002 (SOX) requires senior management of publicly traded companies to both (i) establish and maintain adequate internal controls for financial reporting, and (ii) assess annually the effectiveness of those controls. The law also establishes attestation requirements for public accounting firms to assess management's certification of the effectiveness of its internal controls over financial reporting.[1]

Since its passage, SOX has engendered debate within the management and IT community over the extent to which Section 404 addresses the need for appropriate IT security in establishing and maintaining effective internal controls. Much of this debate suggested that the Act was silent on the subject; though there was general agreement among auditors and IT professionals that, silent or not, the Act required -- as a practical matter -- adequate IT security to comply with the internal control provisions of Section 404.

Intrigued by this debate and its potential implications for its members and the business community generally, the Cyber Security Industry Alliance (CSIA) commissioned a study to determine whether compliance with Section 404 "requires" effective information security.[2] In conducting this study, CSIA examined the specific provisions of the statute passed by Congress, in addition to a number of other legally relevant materials essential to interpreting Section 404.[3] Upon review of these materials the study concluded that compliance with Section 404 of SOX does require publicly traded companies to employ information security to the extent necessary to ensure the effectiveness of internal controls over financial reporting.

In reaching this conclusion, however, the study observed that IT governance and security were given relatively limited treatment in the SOX materials. Of the 216 paragraphs comprising Audit Standard No. 2, only two – paragraphs 50 and 75 -- address the effect of IT on internal controls. Even then, the reader is directed to consult portions of another document published in 2001, Statements of Auditing Standards No. 94 (SAS 94), for substantive guidance. Given the size, complexity, and variety of interdependent functions performed by IT systems and networks in most publicly traded companies, this

[1] §404 of the Sarbanes-Oxley Act of 2002, P.L.-107-204, 116 Stat. 746, codified at 15 USC §§7201, 7262 (2004).
[2] See *Sarbanes-Oxley Act: Implementation of Information Technology and Security Objectives*, Cyber Security Industry Alliance, December 2004.
[3] These include: (i) the rules issued by the Securities and Exchange Commission (SEC) that implement SOX statutory provisions; (ii) the standards issued by the Public Company Accounting Oversight Board (PCAOB) in Audit Standard No. 2 and adopted in rulemaking by the SEC; and (iii) various provisions contained in the Statements of Auditing Standards Nos. 55, 78, and especially 94, issued by the American Institute of Certified Public Accountants (AICPA) and specifically incorporated into Audit Standard No. 2 by the PCAOB and the SEC.

limited treatment raises an important legal and practical question: Do the statutory and administrative materials governing Section 404 provide enough detailed guidance on IT security to enable management and auditors to carry out their respective compliance obligations?

To answer this question, CSIA co-sponsored a conference on May 3, 2005, in Washington, D.C., with George Mason University School of Law's Critical Infrastructure Protection Program (GMU), The Institute of Internal Auditors (IIA), the Information Systems Audit and Control Association (ISACA), and the Information Systems Security Association (ISSA).

The by-invitation-only conference -- *IT Security and Sarbanes Oxley Compliance: A Roundtable Dialogue of Lessons Learned* – consisted of four panels that brought together experts representing each of the key stakeholder communities involved in Section 404 compliance; specifically, corporate management, audit and accounting, legal counsel, and IT security officers and professionals. The audience, which was comprised of over 150 mid- and senior-level professionals from the respective stakeholder communities, was invited to join the dialogue during the question-and-answer sessions that followed each panel discussion.

Each of the panels addressed two general themes:

- Experience and Lessons Learned: What was the experience of senior managers, auditors, legal counsel, and IT officers in addressing the IT security issues necessary to comply with Section 404? Did the standards issued by the Securities and Exchange Commission (SEC) and the Public Company Accounting Oversight Board (PCAOB) provide adequate guidance for companies struggling to comply with SOX for the first time?

- Looking to the Future: Do these stakeholders want or need more detailed guidance on IT now that they have gone through the SOX process? Has the accumulated experience and capabilities gained by companies and accounting firms during their first time through the SOX process render additional PCAOB guidance unnecessary or undesirable? What form would additional guidance take? What would such guidance seek to achieve? What benefits and risks would they present to stakeholders?

This report summarizes the key findings and conclusions arising from these panel discussions, as well as the question and answer sessions. Although much discussion concerned the general experience of SOX compliance, this report covers only those aspects of the dialogue that were specifically related to IT security.

Finally, though the findings and conclusions of this report attempt to capture the views expressed during the conference, they do not necessarily represent the views of the sponsoring organizations. Moreover, while this report contains some of the policy prescriptions occasionally proffered by panelists and audience participants during the

roundtable discussion, it does not, by including them here, necessarily suggest that the sponsoring organizations either advocate or recommend their adoption.

The Afterword provided at the end of the report discusses the implications for Section 404 compliance of two developments that occurred shortly after the Conference; specifically, the statement by the SEC on internal controls and information technology, and the spate of widely reported identify theft and fraud incidents involving publicly traded companies.

II. Key Findings

A. Steep Learning Curve Was Inevitable Regardless of Adequacy of IT Guidance

The passage of SOX was intended to and was viewed by the leaders of publicly traded companies as a "shot across the bow" – a warning that scandals such as Enron and MCI/WorldCom would not be tolerated and that chief executive officers personally would be held criminally liable for failing to exercise proper corporate probity in the future. The heated political climate that led to SOX, combined with the bright spotlight directed at corporate leaders with each new revelation of scandal, mismanagement, or fraud, virtually assured that the first round of SOX compliance was going to entail a "steep learning curve."

Against this backdrop, companies approached their compliance task with extreme care and due diligence. In general, companies tended to (i) focus their efforts on "low hanging fruit" (i.e., address obvious governance and accounting problems that might raise compliance and liability questions), and (ii) invest large sums in consulting services because they either lacked the in-house resources to manage the compliance process themselves or wanted added insurance that they were doing the right things in the right way.

Some companies focused on short-term fixes – "Band-Aids" -- to meet SOX compliance requirements, while others used the opportunity presented by SOX to establish and institutionalize more effective processes and controls. The absence of segregation of duties significantly complicated overall compliance efforts for some companies (especially smaller public companies), including addressing IT governance and security matters relating to internal controls.

Several panelists noted the lack of detailed IT-related guidance in Section 404 and the need to rely on unofficial sources (see discussion below) to aid their compliance efforts; but given the political and economic climate in which the first round of SOX compliance took place, most of the panelists seemed to agree that even with more detailed official guidance on IT, the process of complying with Section 404 was inevitably going to be difficult and challenging.

B. IT Security Not CEO Priority

SOX received considerable attention and oversight from chief executives. Some panelists saw the degree of CEO attention given to SOX in some ways analogous to the Y2K experience, when the SEC required CEOs to certify publicly the extent to which their companies were Y2K compliant. In both cases: (i) the CEO was accountable and had to "sign his name on the dotted line," (ii) there was a "hard" compliance date to meet, and (iii) "failure" to comply posed potentially damaging consequences for corporate reputation and brand. Additionally, SOX carried the risk of personal liability of senior management and directors.

However, unlike the Y2K experience, where IT was understood by senior management to be at the heart of their SEC disclosure requirement, the relationship between IT and compliance under Section 404 was not well understood by senior management and, thus, not generally given personal priority attention. To the extent IT was considered at all by senior management, it was viewed as a technical matter to be delegated and addressed by the IT department and/or the auditors.

There are a number of reasons for this relative lack of attention. As stated before, the law of SOX gives very limited treatment of IT, as compared to other matters covered by the Act. The subject was never debated in Congress prior to the law's passage. CEOs listen to what Congress says and what lawmakers think is important. Congress was silent on IT. By contrast, the Y2K legislation that required the SEC disclosures was overtly and obviously about IT matters. Chief executives heard the message and acted accordingly.

Another reason for the relative lack of CEO attention to IT governance and security was that the relationship between the concept of "internal controls" and the role of IT security was not well recognized by corporate leaders. "Internal controls" is an accounting concept; IT security is still mainly considered a technical, rather than a business, matter. Given the vast issues of SOX compliance that CEOs had to attend to personally, the general view was to let the IT departments deal with the "technical" problem. In this regard, according to some panelists, management probably overestimated the ability and knowledge of IT departments to translate assessments of adequacy of IT systems into terms of adequacy of "internal controls" for purposes of SOX compliance.

Looking to the future, the panelists generally agreed that CEO attention to IT security will likely increase with improved synergy between internal controls, IT security, and the chief executive's ability to comply with assessment obligations. CEOs must also gain a clearer understanding of the legal implications of that synergy in order to more fully appreciate the importance of IT security.

C. Deference to Auditors by Management and Legal Counsel

Compliance with Section 404 under SOX is inherently a legal matter; the law was designed to hold management and auditors separately accountable, thus creating a deliberate tension of interests. Nevertheless, both management and legal counsel tended

to defer to the auditors, internal and external, as regards interpreting and implementing SOX standards with respect to Section 404 compliance.

There were a number of reasons for this deference. SOX and its supporting administrative materials were viewed as written for and directed mainly at auditors. Management and corporate counsel usually were not conversant in the language or concepts contained in Section 404, such as the meaning and application of "internal controls," which are crucial to SOX interpretation and compliance. More importantly, management believed that the auditors were in the best position to interpret compliance requirements: corporate executives knew that the auditors were ultimately responsible for passing on the sufficiency of internal controls; hence the use of audit firm consultants to "pre-clear" internal controls before the "real" audit under Section 404(b) was conducted. In addition, audit firms' development of their own internal guidance further led companies to rely on that guidance to pass the auditor's scrutiny. Under these circumstances, management usually did not seek legal counsel's opinion and analysis on matters beyond those such as "material weakness," which could lead to litigation. Nor did legal counsel, according to some panelists, necessarily seek to assert a greater role in Section 404 compliance apart from such matters.

Auditors did not always welcome this deference. According to several panelists, auditors tended to believe that management is in a much better position to understand their general systems of controls, and which of those are critical to the production of financial reports. The management team is also in a better position, according to these panelists, to understand which IT systems and security architectures operate or otherwise affect those systems of controls. In their opinion, SOX is about integrity in the financial reporting process, which is mainly about management; auditing is simply the means of affirming that adequate controls are in place to achieve those objectives.

D. Augmentation of COSO Framework Required

Under Section 404 of SOX, assessments regarding the effectiveness of a public company's internal controls must be based on "a suitable, recognized control framework established by a body of experts that followed due-process procedures." The PCAOB identified the framework established in the document *Internal Control – Integrated Framework*, published by the Treadway Commission's Committee of Sponsoring Organizations (COSO Framework), as suitable for purposes of Section 404, and, for that reason, it would serve as the basis for the performance and reporting standards set forth in Audit Standard No. 2, which is the standard adopted by the SEC for purposes of Section 404 compliance.

Both auditors and IT professionals indicated that the COSO framework alone provided insufficient guidance to enable them to carry out their Section 404 compliance obligations. To augment the COSO framework for purposes of assessing IT security controls, some auditors and IT professionals referred to the standard set forth in the *Control Objectives for Information and related Technology* (COBIT), developed by ISACA's IT Governance Institute. COBIT was developed as a generally applicable and

accepted standard for IT security and control practices that provides a reference framework for management, users, and IS audit, control and security practitioners. A number of panelists advocated formal recognition by the PCAOB of COBIT as an example of a standard that can provide further guidance on IT governance and security. (This recommendation is discussed below in more detail in Section III.A.) However, some found COBIT still too broad and not sufficiently focused on financial controls; many of them turned to the IT Governance Institute's adaptation of COBIT for Section 404 compliance[4] as an alternative to the general COBiT standard.

An alternative approach, expressed by a number of panelists, was for publicly traded companies to augment the COSO framework with the use of one of the recognized international standards for IT security, such as the so-called "British standard" or ISO 17799. Such an approach would, according to these panelists, not only reduce the uncertainties of Section 404 compliance arising from the COSO framework, but also address the problems of international competition that could arise from adopting separate standards for SOX compliance. Specifically, a separate IT standard for SOX could potentially place U.S. publicly traded companies at a competitive disadvantage vis-à-vis non-U.S. companies that are not subject to the law. Adoption of an international standard would level the playing field as well as provide the necessary assistance to U.S. public companies in complying with Section 404.

E. Existing Control Processes and Procedures Affected SOX Compliance Activities

While it can hardly be said that publicly traded companies welcomed the passage of SOX, some were in a better position to meet their Section 404 compliance obligations than others. Those that already established and implemented solid internal controls throughout their organization found the SOX compliance experience relatively "painless."

For example, under Section 404, management is expected to document and test relevant general IT controls in addition to appropriate application-level controls that are designed to ensure that financial information generated from a company's application systems can reasonably be relied upon. If companies had established and instituted generally effective documentation policies and procedures, IT departments tended to do the same, greatly facilitating assessments of IT controls, including security. This was especially the case where IT was aligned with the business strategy of the company – documentation became "easier" to audit because it closely tracked financial goals and IT goals.

Companies that did not have in place well established controls were confronted with a more complicated and arduous audit and compliance process. Some of the problems reported by panelists included: lack of proper segregation of duties and responsibilities essential to demonstrating the integrity of financial reporting; absence of consistent and

[4] *IT Control Objectives for Sarbanes-Oxley, the Importance of IT in the Design, Implementation, and the Sustainability of Internal Control Over Disclosure and Financial Reporting*, IT Governance Institute (2004), reprinted at http://www.isaca.org/.

integrated approaches to user access of IT systems; inadequate processes and procedures that, therefore, required companies to resort to ad hoc remedies to address their near-term compliance challenges; lack of understanding of how IT controls relate to internal controls complicated the testing of the adequacy of those controls by IT departments. Indeed, officials responsible for IT governance and security -- i.e., CIO, CSO, CISO -- reported that activities related to SOX compliance tended to consume considerably more time than expected, often at the expense of performing their other duties and/or funding other IT efforts.

III. Conclusions and the Future

A. Need for Additional IT Security Guidance from PCAOB?

The panelists were split on the question of additional guidance. Representatives of management and legal counsel generally opposed additional guidance from PCAOB on IT governance and security. Such guidance was deemed unnecessary (because the accumulated experience and capabilities gained by companies and accounting firms during their first time through the SOX process were sufficient to handle future IT compliance challenges); unhelpful (because public companies are too diverse in size, complexity, and operations, for a "one-size-fits-all" solution); and unwanted (because more detailed guidance would effectively create additional regulation and, potentially, greater standards of duty and care).

Representatives of the public accounting firms indicated that they needed and were seeking additional guidance on some aspects of IT controls, such as benchmarking and baselining; application control testing; and standardization of some of the standards set forth in Audit Standard No. 2. A number of panelists advocated formal recognition by the PCAOB of COBiT as an example of a framework that management and auditors can refer to for additional guidance on IT governance and security. They noted that COBiT is widely used, is the product of a body of experts that followed due process procedures, is sufficiently broad to enable companies to tailor the framework to their specific needs, and, therefore, is fully consistent with the SEC's present guidance on IT and internal controls.

B. Evolving Legal Issues and Role of Legal Counsel

Most panelists indicated that legal counsel is likely to reassert itself in Section 404 compliance matters in the future. In the final analysis, SOX is a law that must be understood by legal counsel in order to provide essential advice to senior management. However, at least one panelist observed that the limited role of legal counsel established by management during the first round of SOX compliance may continue for the reasons set forth above in Section II.C (i.e., that management will continue to rely on auditors for compliance matters given their ultimate role in certifying the effectiveness of internal controls, while turning to legal counsel when questions arise over matters of material weakness or circumstances that could lead to litigation).

Several panelists observed that the audit standards and controls covered under the COSO framework could become legal standards of care for courts to assess the degree to which reasonable judgment was exercised by senior management in carrying out their Section 404 obligations.

Panelists also observed that IT governance and security are likely to become more prominent legal issues during Section 404 compliance reviews. The relationship between developing and maintaining internal controls and IT security -- especially access controls and strong authentication -- is likely to be understood and receive greater attention by senior management in the future.

Document retention requirements are likely to come to the forefront of legal counsels' concerns. SOX-relevant documents must be retained for possible litigation. As one panelist noted, IT systems will be considered the most reliable witness when it comes to data retention. Courts will have to understand better the role IT plays in SOX compliance. The challenge for companies and counsel will be deciding which documents are relevant and must be retained, and establishing effective processes and procedures to ensure those decisions are understood and applied at all levels of the company.

C. Common Framework and Lexicon Among Stakeholder Communities

Panelists were unanimous in the view that the various stakeholder communities did not understand or communicate with each other effectively with respect to Section 404 compliance, generally, and IT governance and security, specifically. Each community communicated in terms and language unique to their profession, expecting the others to understand the meaning and application of the underlying concepts.

While most panelists opposed additional guidance by PCAOB, all agreed that a common lexicon and conceptual framework on IT governance and security is needed to create a sustainable Section 404 compliance process and to ensure that all stakeholders were working from a common understanding of each other's roles and responsibilities in implementing that process.

How such a lexicon and conceptual framework would be developed and who would organize the effort was not discussed. However, should the management, audit, and legal counsel communities decide to organize such an effort, CSIA is prepared to provide whatever technical assistance on IT security is required to advance the project's goals and objectives.

* * *

AFTERWORD

Two developments occurred shortly after the Conference which bear directly on IT security and SOX compliance, and which a number of conference participants requested be included in this report as an Afterword.

The first development occurred on May 16, 2005, when the SEC issued a Staff Statement[5] indicating that it would not prescribe additional standards on matters relating to IT controls and Section 404 compliance. Instead, the Commission would look to management to exercise appropriate discretion and judgment in carrying out its compliance obligations.

Specifically, the SEC stated that it never intended Section 404 to be a "one-size-fits-all" approach to assessing controls and, therefore, believed it was not possible for the Board to provide an exact list of the general IT controls that should be included in an assessment for Section 404 purposes.[6] The Commission also recognized that companies were using proprietary IT frameworks as a guide to conducting the IT portion of their overall COSO framework assessment, and supported the use of such proprietary frameworks, in whole or in part, so long as management applies reasonable judgment and considers the impact of IT systems on internal controls over financial reporting.[7]

Based on these statements, it would appear that more specific guidance from the PCAOB on IT controls is unlikely in the near future. That said, a couple of conference participants observed that formal recognition of COBIT by the SEC would be fully consistent with its position to encourage management discretion and judgment and avoid dictation of specific IT controls through detailed checklists.

The second development occurred over a number of weeks and involved several highly reported breaches of privacy of customer information by publicly traded companies. In response, the Congress has indicated that legislation is likely in 2005 to require companies to report such breaches and to undertake steps to better secure customer data against unauthorized use. A number of conference participants identified two potential implications for SOX and IT security should legislation along these lines pass. First, that such legislation, if past precedent is any guide to the future, is likely to be considered and adopted by Congress without sufficient consideration given to its consistency with other laws on the books, such as Section 404 of SOX, and certainly with respect to IT governance and security. Second, should the legislation detail specific provisions on IT security, similar provisions may be imposed on SOX down the road. At a minimum, such provisions are likely to strongly influence the way in which IT security is implemented to comply with Section 404. According to these conference participants, both implications may warrant more proactive action by the stakeholder communities to inform the legislation on customer privacy, as well as revisit the need for more explicit clarity by the SEC on IT security under SOX.

---

[5] *Staff Statement on Management's Report on Internal Control Over Financial Reporting,* Securities and Exchange Commission, May 16, 2005.
[6] *Id.*
[7] *Id.*

ABOUT THE CYBER SECURITY INDUSTRY ALLIANCE

The Cyber Security Industry Alliance is an advocacy group to enhance cyber security through public policy initiatives, public sector partnerships, corporate outreach, academic programs, alignment behind emerging industry technology standards and public education. Launched in February 2004, the CSIA is the only public policy and advocacy group comprised exclusively of security software, hardware and service vendors that is addressing key cyber security issues. Members include BindView Corp.; Check Point Software Technologies Ltd.; Citadel Security Software Inc.; Citrix Systems, Inc., Computer Associates International, Inc.; Entrust, Inc.; Internet Security Systems Inc., iPass, Inc., Juniper Networks, Inc., McAfee, Inc., PGP Corporation; Qualys, Inc.; RSA Security Inc.; Secure Computing Corporation, Surety, Inc., Symantec Corporation, and TechGuard Security.

Cyber Security Industry Alliance
2020 North 14th Street N.
Suite 750
Arlington, VA 22201
(703) 894-CSIA
www.csialliance.org