CYBER SECURITY
INDUSTRY ALLIANCE

Sarbanes-Oxley Act: Implementation of Information Technology and Security Objectives

December 2004

Executive Summary

Since its passage, the Sarbanes-Oxley Act of 2002 (SOX) has engendered considerable debate over the law's implications for corporate information security, especially the case with respect to the internal control provisions of Section 404.

Section 404 of SOX requires senior management of publicly traded companies both to (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.

In determining whether compliance with Section 404 "requires" effective information security, one has to examine, in addition to the specific provisions of the statute passed by Congress, a number of other legally relevant materials. 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.

Review of the these statutory and administrative materials clearly indicates that compliance with Section 404 of SOX requires publicly traded companies to employ information security to the extent necessary to ensure the effectiveness of internal controls over financial reporting. The SEC and PCAOB explicitly recognize the potentially adverse effects of IT on internal controls; regulators also, in effect, impose a duty on senior management to secure their corporate IT systems to the extent necessary to ensure the accuracy and integrity of such reporting.

In reaching this conclusion, we recognize that, given the size and complexity of IT systems and networks in most publicly traded companies, the statutory and administrative materials governing Section 404 may still lack the detail and specificity regarding IT governance and security that management and auditors might want to guide and inform their compliance efforts. This raises a number of objective questions: Does management and/or the audit community indeed want or require more detailed and specific guidance on how companies may meet Section 404 compliance requirements for information security? Should PCAOB be asked to provide such guidance? Is additional legal guidance needed or desirable? If not, how can management and auditors conduct Section 404 activities more efficiently and effectively?

Action. CSIA should release its findings and announce a summit of senior managers, auditors, and IT professionals to explore issues discussed in this paper. The summit would also consider whether additional guidance is necessary from the Federal government or professional organizations. The summit will be held in during the Spring of 2005.

I. Introduction

Since its passage, the Sarbanes-Oxley Act of 2002 (SOX)[1] has engendered considerable discussion and debate over the law's implications for corporate information security, especially with respect to compliance with the internal control provisions of Section 404. Much has been written in professional publications about the lack of clear and specific guidance on these matters in the statutory and administrative materials and the need to supplement these materials with others, such as COBIT, to enable independent auditors to fulfill their obligations under Section 404.[2]

In doing so, these efforts have tended to blur the distinction between law and practice. Yet understanding the extent to which the law "requires" IT security is important, not only to auditors, but also for corporate managers. To the extent there are obligations to secure IT systems in order to comply with Section 404, then there are implied liabilities for failing to do so. Moreover if the contours of that liability are amorphous or ill defined, then management could be exposed to considerable legal risk for failing to consider IT security as part of a compliance strategy.

This paper explores the extent to which SOX requires IT security for purposes of Section 404 compliance. Based on our review of the relevant statutory and administrative authorities, we conclude that the law requires corporate management and the audit profession to consider IT security as part of core compliance requirements. We specifically conclude that IT security risk may affect various components of both management's certification and auditor attestation and outline relevant standards recognized by lawmakers in addressing Section 404 responsibilities.

This examination entails several inquiries. First and foremost, we consider how various parts of the law – statutory, regulatory, and administrative – connect with regard to information security. This review involves assessing statutory directives on internal controls as well as regulatory and administrative commentary, including guidance published by the Public Company Accounting Oversight Board (PCAOB) relating to information technology risks. Finally, we highlight specific language in standards directly affecting review of internal controls and information technology. When read together, these materials pinpoint obligations for publicly traded companies to secure those IT systems essential for the integrity of financial reporting.

---

[1] Sarbanes-Oxley Act of 2002 (H.R. 3763), Pub Law 107-204 (2002), 116 Stat 145, codified at 15 USCA §7201 et seq.

[2] Refer, for example, to the *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/.

II. Road Map of the Law: Sarbanes-Oxley Act and Implementation Guidance

Congress adopted SOX, and Section 404 in particular, to protect investors and shareholders by ensuring the integrity of financial reporting and forcing corporate officials to undertake full responsibility for public disclosures required under the law. Congress integrates these philosophic principles throughout the statute and directs the PCAOB to develop appropriate standards to oversee implementation.

As a result, whether and the extent to which Section 404 requires information security is a function of how the Securities and Exchange Commission (SEC), the PCAOB, and other authorities implement the law. The box below lists many of the relevant authorities that are part of the analysis:

Information Security and Sarbanes-Oxley: Authoritative Material

- ✓ The provisions of the statute passed by Congress
- ✓ The rules issued by the Securities and Exchange Commission (SEC) that implement those statutory provisions
- ✓ Formal criteria issued by the Public Company Accounting Oversight Board (PCAOB) in Audit Standard No. 2 and adopted in rulemaking by the SEC
- ✓ Commentary and additional guidance published by the PCAOB on how the standard requires consideration of IT risks
- ✓ Various provisions of Statements of Auditing Standards Nos 55, 78, and especially 94 (SAS 94) issued by the American Institute of Certified Public Accountants and cited/incorporated into Audit Standard No. 2 by the PCAOB and the SEC

a. The Statute

Section 404 of the Sarbanes-Oxley Act is the core provision for analyzing how SOX mandates information technology and security considerations. The statute requires senior management both to establish and maintain adequate internal controls for financial reporting, and to assess annually the effectiveness of those controls. It also establishes attestation requirements for public accounting firms to assess management's certification of the effectiveness of its internal controls over financial reporting.

Key Provisions in Sarbanes-Oxley

Specifically, Section 404 provides:

Rules Required. – The [Securities and Exchange Commission] shall prescribe rules requiring each annual report required by . . . the Securities Exchange Act of 1934 . . . to contain an internal control report, which shall –

1. *state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and*
2. *contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.*

Internal Control Evaluation and Reporting. – With respect to the internal control assessment required by subsection (a), each registered public accounting firm that prepares or issues the audit report for the issuer shall attest to, and report on, the assessment made by management of the issuer. An attestation made under this subsection shall be made in accordance with standards for attestation engagements issued or adopted by the [Public Company Accounting Oversight Board]. Any such attestation shall not be subject of a separate engagement.[3]

Congress' decision to create a standards-setting organization is important for understanding how the law integrates information security requirements. SOX creates a PCAOB responsible for issuing audit standards to enable public accounting firms to carry out their attestation obligations.[4] These standards are law when approved and adopted by the Securities and Exchange Commission (SEC), which retains overall rule-making authority under SOX.

3 §404 of the Sarbanes-Oxley Act of 2002, P.L.-107-204, 116 Stat. 746, codified at 15 USC §§7201, 7262 (2004).

4 Title I of Sarbanes-Oxley creates the PCAOB and provides for its jurisdiction (15 USC § 7211). This includes and responsibility to oversee the audit of public companies subject to the securities laws.

b. Administrative Rulings Implementing SOX – Audit Standard No. 2

Almost immediately after Congress adopted the SOX, the newly created PCAOB embarked on a formal process to define compliance criteria for Section 404. In July 2003, the PCAOB Staff issued a briefing paper on its intentions with regard to SOX requirements relating to internal controls.[5] That paper was used as a basis for a roundtable discussion between the PCAOB, corporate compliance specialists, public auditing professionals, and others. All of the stakeholders, both public and private, engaged in formal discourse over the meaning of internal controls in the context of the statute, whether the Committee of Sponsoring Organizations (COSO) should serve as a foundation for compliance, and what other activities would be essential for compliance with the law.

The stakeholders did not dwell on IT governance or security in the initial meetings and briefings by the PCAOB. Rather, those meetings, and the material resulting form the discussions, focused more on the broader legal and regulatory concepts – mostly covering internal control definitions and practices as well as PCAOB expectations for the auditing profession.

In March 2004, the PCAOB completed its extensive review of options and issued the Audit Standard No. 2 to implement the provisions of Section 404.[6] In June 2004, it became law by order of the SEC.[7]

---

5 Public Company Accounting Oversight Board, *Briefing paper for the Roundtable on Reporting on Internal Control* (July 10, 2003), reprinted at http://www.pcaobus.org/rules/2003-07-10_Internal_Control_Briefing_Paper.pdf

6 Auditing Standard No. 2, *An Audit of Internal Control Over Financial Reporting Conducted in Conjunction With an Audit of Financial Statements* (heretofore referred to as “Auditing Standard No. 2”) (March 9, 2004).

7 SEC, Release No. 34-49884; File No. PCAOB 2004-03, Public Company Accounting Oversight Board; Order Approving Proposed Auditing Standard No. 2, An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements ("Auditing Standard No. 2") (June 17, 2004) reprinted at SEC Notice of Order http://www.sec.gov/rules/pcaob/34-49884.htm

c. PCAOB Defines Expectations for Internal Control: Commission's Committee of Sponsoring Organizations is Principal Framework

After receiving recommendations and suggestions from a wide range of corporate interests, PCAOB settled on an official definition of internal controls for purposes of SOX compliance. Specifically, "internal controls over financial reporting" are defined as:

> *A PROCESS DESIGNED BY, OR UNDER THE SUPERVISION OF, THE COMPANY'S PRINCIPAL EXECUTIVE AND PRINCIPAL FINANCIAL OFFICERS, OR PERSONS PERFORMING SIMILAR FUNCTIONS, AND EFFECTED BY THE COMPANY'S BOARD OF DIRECTORS, MANAGEMENT, AND OTHER PERSONNEL, TO PROVIDE REASONABLE ASSURANCE REGARDING THE RELIABILITY OF FINANCIAL REPORTING AND THE PREPARATION OF FINANCIAL STATEMENTS FOR EXTERNAL PURPOSES IN ACCORDANCE WITH GENERALLY ACCEPTED ACCOUNTING PRINCIPLES AND INCLUDES THOSE POLICIES AND PROCEDURES THAT:*
>
> 1. *Pertain to the maintenance of records that, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the company;*
> 2. *Provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the company are being made only in accordance with authorizations of management and directors of the company; and*
> 3. *Provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the company's assets that could have a material effect on the financial statements.*[8]

Building on this core concept, Audit Standard No. 2 then requires management to base its Section 404 assessments of the effectiveness of its company's internal controls on "a suitable, recognized control framework established by a body of experts that followed due-process procedures."[9] 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, would serve as the bases for the performance and reporting standards set forth in Audit Standard No. 2.[10]

The COSO Framework identifies three objectives for internal control: (1) efficiency and effectiveness of operations; (2) reliability of financial reporting; and (3) compliance with applicable laws and regulations.[11] In adopting this framework, the PCAOB indicates that primary attention would necessarily be given to the second of the three objectives listed – *i.e.*, ensuring the reliability of financial reporting -- but quickly cautioned against any preemptory exclusion of the other two control objectives:

> *. . . all controls that materially affect financial reporting, including controls that focus primarily on the effectiveness and efficiency of operations or compliance with laws and regulations and also have a material effect on the reliability of financial reporting, are a part of internal control over financial reporting.*[12]

---

[8] Auditing Standard No. 2 at paragraph 7. Throughout the standard, internal control over financial reporting (singular) refers to the process described in this paragraph. Individual controls or subsets of controls are referred to as controls or controls over financial reporting.

9 *Id* at para 13.

10 *Id* at para 14.

11 *Id* at para 15. For background on the *COSO Internal Control – Integrated Framework*, refer to the COSO website at http://www.coso.org/. Both accounting and security practitioners have focused significant energies on the COSO framework since passage of the Sarbanes-Oxley Act, although for somewhat different purposes. The language of "internal controls," and the relevance of internal controls to enterprise security, is fully explored in the COSO's *Enterprise Risk Management Framework*, which is currently being reviewed. For background analysis on the ERM Framework, refer to *Information Security Governance, A Call to Action* (August 2004).

12 *Id*.

To achieve these objectives, an entity's internal controls should be developed and maintained in a manner that ensures each of five components is appropriately addressed. They are described as follows:

1. **Control environment** sets the tone of an organization, influencing the control consciousness of its people.
2. **Risk assessment** is the company's identification and analysis of relevant risks to achievement of its objectives, forming a basis for determining how the risks should be managed.
3. **Control activities** are the policies and procedures that help ensure that management directives are carried out.
4. **Information and communication** systems support the identification, capture, and exchange of information in a form and time frame that enable people to carry out their responsibilities.
5. **Monitoring** is a process that assesses the quality of internal control performance over time.[13]

The COSO Framework has enjoyed wide acceptance within the audit community well before the passage of SOX. Its adoption by the PCAOB and SEC was not, therefore, surprising. The COSO Framework establishes a foundation for sound corporate governance, including the establishment and maintenance of IT controls. That said, the framework, as published by the Treadway Commission, does not provide the level of guidance needed to ensure compliance with Section 404, specifically, or the achievement of effective IT governance, generally.

13 The five components of the COSO framework in Statement on Auditing Standards No. 55, *Consideration of Internal Control in a Financial Statement Audit*, AICPA, Professional Standards, vol. 1, AU sec. 319.

III. SOX Compliance and IT Guidance – Statement on Auditing Standards (SAS) 94

Throughout its analysis, the PCAOB recognizes both the potential impact of IT on the effectiveness of internal controls over financial reporting and the limits of the COSO framework in providing the guidance needed to appropriately address that impact. In paragraph 75 of the Audit Standard No. 2, the PCAOB states that "[t]he nature and characteristics of a company's use of information technology in its information system affect the company's control over financial reporting."[14]

To explain how this might happen and what the potential consequences might be for the establishment and maintenance of internal controls, the PCAOB incorporated portions of the Statement on Auditing Standards No. 94 (SAS 94) issued by the American Institute of Certified Public Accountants (AICPA).[15] SAS 94 provides "guidance on the independent auditor's consideration of an entity's internal control in an audit of financial statements in accordance with generally accepted auditing standards." In doing so, it recommends that auditors understand how the use of IT can affect the five internal control components set forth in the COSO Framework:

> *An entity's use of IT may affect any of the five components of internal control relevant to the achievement of the entity's financial reporting, operations, or compliance objectives, and its operating units or business functions. For example, an entity may use IT as a part of discrete systems that support only particular business units, functions, or activities, such as a unique accounts receivable system for a particular business unit or system that controls the operation of factory equipment. Alternatively, an entity may have complex, highly integrated systems that share data and are used to support all aspects of the entity's financial reporting, operations, and compliance objectives.*[16]

Most important for purposes of this paper, the sections of SAS 94 incorporated into Audit Standard No. 2, and thus SOX, explicitly recognize the role and importance of IT security in ensuring effective internal controls. Paragraphs 18 and 19 of SAS 94 discuss the benefits and risks of IT on internal controls, respectively. With respect to the benefits, the Statement states that -

> *IT provides potential benefits of effectiveness and efficiency for an entity's internal control because it enables an entity to --- [among other things]*
>
> - *Enhance the ability to achieve effective segregation of duties by implementing security controls in applications, databases, and operating systems."*[17]

With respect to the risks, SAS 94 states:

> *IT also poses specific risks to an entity's internal control, including – [among other things]*
>
> - *Unauthorized access to data that may result in destruction of data or improper changes to data, including the recording of unauthorized or nonexistent transactions or inaccurate recording of transactions.*
> - *Unauthorized changes to data in master files.*
> - *Unauthorized changes to systems or programs.*
> - *Potential loss of data.*[18]

---

14 Auditing Standard No. 2 at para 75. See also para 50:

> *Some controls (such as company-level controls . . .) might have a pervasive effect on the achievement of many overall objectives of the control criteria. For example, information technology general controls over program development, program changes, computer operations, and access to programs and data help ensure specific controls over the processing of transactions are operating effectively. . . .*

15 Statement on Auditing Standards No. 94, *The Effect of Information Technology on the Auditor's Consideration of Internal Control in a Financial Statement Audit* (2001) (hereinafter referred to as "SAS 94).

16 *Id* at para 16.

17 *Id* at para 18.

18 *Id* at para 19

The degree to which IT poses a risk to internal controls depends on a number of factors. One such factor is the nature and characteristics of a company's information system. The PCAOB cites this example from SAS 94:

> *The extent and nature of these risks to internal control vary depending on the nature and characteristics of the entity's information system. For example, multiple users, either external or internal, may access a common database of information that affects financial reporting. In such circumstances, a lack of control at a single user entry point might compromise the security of the entire database, potentially resulting in improper changes to or destruction of data.*[19]

Another factor is the extent of IT dependency:

> *Some controls … might have a pervasive effect on the achievement of many overall objectives of the control criteria. For example, information technology general controls over program development, program changes, computer operations, and access to programs and data help ensure that specific controls over the processing of transactions are operating effectively. In contrast, other controls are designed to achieve specific objectives of the control criteria. For example, management generally establishes specific controls, such as accounting for all shipping documents, to ensure that all valid sales are recorded.*[20]

19 *Id* at para 20

[20] Auditing Standard No. 2 at para 50

IV. Additional PCAOB Guidance: Q&A and Conforming Amendments

The PCAOB has published, in addition to formal materials defining Auditing Standard 2, several clarification and guidance documents. These documents underscore the importance of information security principles and considerations as part of SOX compliance.

For example, In June 2004, the PCAOB released Staff Questions & Answers on Auditing Standard 2 implementation.[21] One of the key considerations raised by the auditing profession after release of Standard No. 2 was the extent to which outsourcing activities "are part of a company's internal control over financial reporting," and thus part of a SOX compliance review. Information security is a key consideration in an outsourcing arrangement, especially with regard to integrity issues as well as separation of duties. According to the PCAOB:

According to the PCAOB:

> *Q24. What types of outsourcing activities result in a service organization arrangement addressed by Statement on Auditing Standards ("SAS") No. 70, Service Organizations (AU sec. 324)? What types of outsourcing activities are part of a company's internal control over financial reporting?*
>
> *A24. As described in paragraph .03 of AU sec. 324, a service organization's services are part of a company's information system if they affect any of the following:*
>
> - *The classes of transactions in the company's operations that are significant to the company's financial statements.*
> - *The procedures, both automated and manual, by which the company's transactions are initiated, authorized, recorded, processed, and reported from their incurrence to their inclusion in the financial statements.*
> - *The related accounting records, whether electronic or manual, supporting information and specific accounts in the company's financial statements involved in initiating, authorizing, recording, processing and reporting the company's transactions.*
> - *How the company's information system captures other events and conditions that are significant to the financial statements.*
> - *The financial reporting process used to prepare the company's financial statements, including significant accounting estimates and disclosures.*[22]

The PCAOB dedicates a significant portion of its commentary on when and how outsourcing could affect a company's information systems. Here, too, the PCAOB emphasizes important distinctions on the extent to which corporate relationships with service organizations trigger information system considerations:

> *A.24 (cont.) Paragraph .03 of AU sec. 324 also provides examples of situations in which a service organization's services affect a company's information system.*
>
> *For instance, the trust departments of banks and insurance companies often serve as the custodian of an employee benefit plan's assets, including making investment decisions, maintaining records of each participants account, allocating income amongst participants, and preparing other types of recordkeeping; this type of servicing is a common example of a service organization's services that affect a company's information system. In contrast, AU sec. 324 does not apply to situations in which the services being provided are limited to executing client organization transactions that the client specifically authorizes.* [23]

---

[21] Staff Questions & Answers Public Company Accounting Oversight Board, Auditing Standard No. 2 – Internal Control (June 23, 2004), reprinted at http://www.pcaobus.org/QA_Staff_Internal_Control.pdf/.

[22] *Id* at pages 21-22.

[23] *Id*. The PCAOB offers additional examples to clarify as best as possible how auditors should review complex outsourcing relationships. "For example, a company might outsource actuarial services; however, the nature of the services represents the use of a specialist, and the actuary is not a part of the company's information system. If the service organization's services are part of a company's information system, then they are part of the information and communication component of the company's internal control over financial reporting. In those circumstances, management should consider the activities of the service organization in making its assessment of

In September 2004, the PCAOB adopted amendments to its interim standards that conform the text of the interim standards adopted in April 2003 to the requirements of Auditing Standard No. 2. [24] The conforming amendments seek to assist auditors in performing integrated audits of financial statements and internal control and apply certain concepts developed in Auditing Standard No. 2 to circumstances in which an auditor is engaged solely to audit a company's financial statements.[25]

The conforming amendments explicitly recognize the incorporation of SAS 55, 78, and 94 into Auditing Standard No. 2, thus reaffirming the guidance provided in those materials on the application of the COSO framework and the effect of IT on the internal control over financial reporting.[26]

Finally, in November 2004, the PCAOB released additional Staff Questions & Answers on Auditing Standard 2 implementation.[27] Here, the PCAOB provided additional guidance on how to evaluate the significance of deficiencies in IT general controls when such controls, according to the question "by their nature do not" directly affect a company's financial statements.

According to the PCAOB:

> *Q35. Paragraph 50 of Auditing Standard No. 2 states that some controls might have a pervasive effect on the achievement of many overall objectives of the control criteria. For example, information technology ("IT") general controls over program development, program changes, computer operations, and access to programs and data help ensure that specific controls over the processing of transactions are operating effectively. IT general controls whose design or operation is ineffective would, of course, be deficiencies. The definitions of significant deficiency and material weakness, however, focus on the likelihood and magnitude of financial statement misstatement. IT general controls, by their nature, do not affect a company's financial statements directly. How should the significance of deficiencies in IT general controls be evaluated?*
>
> *A35. To evaluate the significance of a deficiency in IT general controls, the effect of the deficiency on application controls should be evaluated. Application controls can be automated control procedures (for example, calculations, posting to accounts, generation of reports, edits, and control routines) performed by IT. When IT is used to initiate, authorize, record, process, or report transactions or other financial data for inclusion in financial statements, the systems and programs may include automated application controls related to the corresponding assertions for significant accounts or disclosures. Application controls also may be manual controls that are dependent on IT (for example, the review by an inventory manager of an exception report when the exception report is generated by IT). Although IT general control deficiencies do not result in financial statement misstatements directly, an associated ineffective application control may lead to misstatements. Therefore, the significance of an IT general control deficiency should be evaluated in relation to its effect on application controls, that is, whether the associated application controls are ineffective.*
>
> *An application control might be effective even if deficiencies exist in IT general controls. For example, in the presence of deficient program change controls, management and the auditor might be able to determine that, in the circumstances, the relevant application controls were operating effectively as of the date of management's assessment. In this case, the deficiency in IT general controls could be classified as only a deficiency. On the other hand, deficient program change controls might result in unauthorized changes to application controls, in which case the application controls are ineffective. In this case, the ineffective program change controls, combined with the ineffective application controls, should be evaluated in terms of likelihood and magnitude of potential financial statement misstatement. In this manner, the combined effect of the ineffective IT general control and the ineffective application control(s)*

---

internal control over financial reporting, and the auditor should consider the activities of the service organization in determining the evidence required to support his or her opinion." *Id*.

[24] Public Company Accounting Oversight Board, *Conforming Amendments to PCAOB Interim Standards Resulting From The Adoption Of PCAOB Auditing Standard No. 2, "An Audit Of Internal Control Over Financial Reporting Performed In Conjunction With An Audit Of Financial Statements," PCAOB Release No. 2004-008, September 15, 2004, PCAOB Rulemaking Docket Matter No. 014.*

[25] *Id*. at p. 2.

[26] *Id*. at p. A-8.

[27] Staff Questions & Answers Public Company Accounting Oversight Board, Auditing Standard No. 2 – Internal Control (November 22, 2004), reprinted at http://www.pcaobus.org/QA_Staff_Internal_Control.pdf/.

could be classified as either a significant deficiency or a material weakness for both the application control and the related IT general control.

The definitions of significant deficiency and material weakness also contain aggregation concepts: a control deficiency, or combination of control deficiencies, can represent a significant deficiency or material weakness. After an IT general control deficiency has been evaluated in relation to its effect on application controls, it also should be evaluated when aggregated with other control deficiencies. For example, all deficiencies affecting the control environment should be evaluated in the aggregate. Management's decision not to correct an IT general control deficiency and its associated reflection on the control environment, when aggregated with other deficiencies affecting the control environment, could lead to the conclusion that a significant deficiency or material weakness in the control environment exists. . . .[28]

28 *Id* at pages 10-12.

V. Conclusions and Next Steps

Our review of the relevant statutory and administrative authorities indicates that compliance with Section 404 of the SOX requires publicly traded companies to employ information security to the extent necessary to ensure the effectiveness of internal controls over financial reporting. The SEC and PCAOB explicitly recognize the potentially adverse effects of IT on internal controls; regulators also, in effect, impose a duty on senior management to secure their corporate IT systems to the extent necessary to ensure the accuracy and integrity of such reporting.

In reaching this conclusion, we recognize that, given the size and complexity of IT systems and networks in most publicly traded companies, the statutory and administrative materials governing Section 404 may still lack the detail and specificity regarding IT governance and security that management and auditors might want to guide and inform their compliance efforts. 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 SAS 94 for substantive guidance.[29]

This raises a number of questions: Does management and/or the audit community want to need more detailed and specific guidance on how companies may meet Section 404 compliance requirements for information security? Should PCAOB provide such guidance? Is such additional legal guidance from these administrative bodies needed or desirable? If not, how might better clarity and specificity be provided to enable management and auditors to conduct their Section 404 activities more efficiently and effectively?

Next Steps

A CSIA SOX Summit

CSIA could convene a summit of senior management, auditors and IT professionals. During the summit a number of issues and options would be discussed, including:

1. **Request clarification through staff Q & A process**: Participants would explore the need, desirability, and feasibility of seeking clarification on how the PCAOB would analyze more complex compliance issues associated with IT security. This option would examine whether and how leveraging the PCAOB's administrative process could help senior management and audit professionals better understand how information security requirements are part of compliance and assist them in mapping requirements and compliance strategies.
2. **Discuss the advisability of creating an awareness program focusing on SOX IT security compliance:** Given the lack of administrative guidance in the law, both management and public auditing professions may need assistance in developing IT security strategies. Many in the IT security community, such as security professionals, also lack awareness of how IT security risks affect financial reporting, fraud, and other principles set forth in SOX. Finally, the PCAOB may also require support on how IT security affects SOX principles.

---

[29] It is interesting to note that, in adopting by reference only portions of SAS 94 into Audit Standard No. 2, the PCAOB chose not to incorporate sections that actually provide useful discussion about the relationship between IT security and the COSO internal control components. For example, with respect to an entity's control environment, the statement notes:

> *[M]anagement's failure to commit sufficient resources to address security risks presented by IT may adversely affect internal control by allowing improper changes to be made to computer programs or to data, or by allowing unauthorized transactions to be processed.*

In another example, this one dealing with an entity's control activities, the statement observes:

> *The use of IT affects the way that control activities are implemented. For example, when IT is used in an information system, segregation of duties often is achieved by implementing security controls.*

3. **Explore an initiative to prepare guidance on IT security specifically for management**: Like guidance incorporated into SAS 94 for public auditing professionals, this material could provide similar guidance for executing certifications by senior managers to support the CFO and CEO SOX certifications.

While each of these projects could be pursued independently by CSIA, it would be preferable to pursue these in coordination with other key stakeholders.

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 exclusively focused on cyber security policy. Members include BindView Corp.; Check Point Software Technologies Ltd.; Citadel Security Software Inc.; Computer Associates International, Inc.; Entrust, Inc.; Internet Security Systems Inc., Juniper Networks, Inc., McAfee, Inc., PGP Corporation; Qualys, Inc.; RSA Security Inc.; Secure Computing Corporation, Symantec Corporation, and TechGuard Security, LLC.

Cyber Security Industry Alliance

1201 Pennsylvania Avenue, NW
Suite 300 #3011
Washington, DC 20004
202-204-0838
www.csialliance.org