

New York Law Journal



Web address: <http://www.nylj.com>

VOLUME 233—NO. 44

TUESDAY, MARCH 8, 2005

ALM

COMPUTER LAW

BY RICHARD RAYSMAN AND PETER BROWN

Sarbanes-Oxley's §404 and Business Process Outsourcing

When the Sarbanes-Oxley Act, Pub. L. No. 107-204, 116 Stat. 745 (2002) (SOX) became law on July 30, 2002, public companies were faced with the daunting task of complying with sweeping legislation that fundamentally altered corporate governance in areas ranging from financial disclosure to auditing and accounting, among others.¹

With almost three years having passed since its enactment, many corporations have begun to take an increasingly careful look at §404 of the act because of the effect that it may have on the outsourcing components of their businesses.

This article will discuss the impact of §404 on some key areas of business process outsourcing (BPO).

§404

Chief among the provisions of SOX is §404, which, generally speaking, requires management to assess the effectiveness of the company's internal control over financial reporting. Section 404 also contains the added obligation of a firm's independent auditor having to attest to, and report on, the assessment made by the management team. This means that the outside auditor must be satisfied with the internal control system of the company.

In today's business world and global economy, the integrity and reliability of financial data no longer falls solely within the province of a company's corporate department. Indeed, computers and information technology play a critical role in the financial internal control area of most companies, given that most day-to-day financial



Richard Raysman

Peter Brown

applications involve computerized programs that are stored on a company's information technology (IT) network. Accordingly, §404 of SOX is particularly relevant to IT and, in turn, to business process functions that involve financial and accounting information and data in the outsourcing environment. For example, routine tasks (e.g., payroll processing), to slightly more complicated jobs (e.g., processing of sales orders from initial customer contact to shipping) to the handling of sophisticated accounting and auditing functions, are just some of many business process operations that almost always involve computers and information technology in their respective performance.

In the broadest sense of the word, outsourcing is simply the transfer of a business function to an outside entity different than the enterprise transferring the business function, regardless of whether that entity is located in the same town or in a different country (often referred to as "off-shore outsourcing"). With respect to §404 of SOX, the location of the outsourcing service provider is irrelevant, as is the fact that a separate entity is performing the work. The obligations created by §404 are non-delegable and the appropriate corporate managers retain responsibility for ensuring that its requirements are satisfied.

SOX grants the Securities and Exchange Commission (SEC) broad authority to promulgate rules and regulations necessary or appropriate to advance the public interest in furtherance of the act, as well as enforce a significant number of its provisions.² In

addition to the SEC's role with respect to SOX, Title I of the act also establishes a Public Company Accounting Oversight Board (PCAOB). The PCAOB, which is not a government agency, but rather a nonprofit corporation, is responsible for overseeing the auditing of public companies that are subject to the securities laws and related matters, including the issuing of accounting standards. The SEC maintains oversight of and enforcement authority over the PCAOB.

The PCAOB has squarely addressed the issue of the duties of §404 being nondelegable, stating "the use of a service organization does not reduce management's responsibility to maintain effective internal control over financial reporting."³ Furthermore, according to the PCAOB, "if the service organization's services are part of the company's information system, ... then they are part of the information and communication component of the company's internal control over financial reporting."⁴ In such a case, management should consider and evaluate controls at the service organization, as well as related controls at the company, when making an assessment about internal control over financial reporting. In addition, the auditor should consider the activities of the service organization when determining the evidence required to support his opinion.⁵ Finally, the SEC has stated, "In situations where management has outsourced certain functions to third-party service provider(s), management maintains a responsibility to assess the controls over the outsourced operations"⁶

Threshold Issue

To trigger §404 in the outsourcing context, a corporation must first determine whether a particular service provider is considered to be part of a company's internal control over financial reporting. This determination was made easier on June 17, 2004, when the SEC approved the PCAOB's Auditing Standard No. 2,⁷ which was released several months earlier on March 9, 2004. With the SEC's

Richard Raysman and **Peter Brown** are partners at Brown Raysman Millstein Felder & Steiner. They are co-authors of "Computer Law: Drafting and Negotiating Forms and Agreements" (Law Journal Press, lawcatalog.com). **Poojitha Rao**, an associate at the firm, assisted in the preparation of this article.

approval, the standard is now effective for audits of internal control over financial reporting required by §404(b) of the act.

Offering further clarification on this issue, the PCAOB has stated that service organizations are part of a company's information system if they affect any of the following: (1) the classes of transactions in the company's operations that are significant to the company's financial statements; (2) the procedures, both automated and manual, by which the company's transactions are initiated, authorized, recorded, processed, and reported from their inurrence to their inclusion in the financial statements; (3) the relating 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; (4) how the company's information system captures other events and conditions that are significant to the financial statements; or (5) the financial reporting process used to prepare the company's financial statements, including significant accounting estimates and disclosures.⁸

Although not an absolute safeguard, the Statement on Auditing Standards (SAS) No. 70, an industry-recognized auditing standard established by the American Institute of Certified Public Accounts (AICPA) in the early 1990s, may offer reasonable assurance that a provider's internal controls comply with §404. An SAS 70 report is often issued in connection with an examination of financial statements of a service provider that has performed business process functions on behalf of another entity. Generally speaking, an SAS 70 audit demonstrates that an independent auditor has thoroughly examined a service provider's internal controls, which quite often may include information technology and related business processes.

There are two types of SAS 70 reports: Type I and Type II. A Type I report is essentially a description of the service provider's internal controls at a specific point in time, while a Type II report includes a description of the provider's internal controls, along with detailed testing of the operating effectiveness of those controls over a period of time, which must be a minimum of six months. The Type II report is more comprehensive, and as a matter of practice, it is generally a better tool to help ensure SOX compliance because of the additional testing requirement for which it provides. The SEC, in fact, appears to have accepted Type II reports as an acceptable method for management's use in §404 compliance, having stated in the context of a question involving third-party service providers that "... Management would be able to rely on the Type 2 SAS 70

report. ..."

The benefits of an SAS 70 audit can reach beyond the corporation, extending to the service provider as well. For example, a service provider's willingness to consent to an SAS 70 audit can speak to the organization's overall reputation, and perhaps even serve as a competitive advantage over other providers that are unwilling to agree to the performance of such an audit.

In addition, positive results of an SAS audit can serve to demonstrate solid and secure internal financial controls in the provider's business or furnish the provider with an opportunity to correct any unknown weaknesses or shortcomings in its operational effectiveness, thereby resulting in an opportunity to improve the overall quality of its services.

Some Caveats

Despite its benefits, companies still need to be aware of certain issues that may arise concerning SAS 70 audits.¹⁰ First, it is important to bear in mind that service providers are not legally required to perform SAS audits and issue SAS 70 reports at the request of a customer. For this reason, a company may wish to include a provision in its contract requiring its service provider to conduct an SAS 70 audit and issue the necessary report.

In addition, the customer should define the scope of the audit, so as to ensure that as much of the service provider's audit is revealed, not just the results of failed tests. When to issue the report is a key component of such a provision. It is generally a good idea to have a report issued that covers the appropriate period of time of the management's required §404 assessment, or, if possible, to have updates to reports issued on a scheduled basis throughout the year. Finally, a corporation should consider choosing a service provider that is willing to have the company's own, separate auditors review any SAS 70 as an added risk management and quality control tool.

Another issue affecting §404 compliance that may escape corporate officers and managers is situations involving the use of subcontractors by service providers that affect financial reporting or internal control activities. Increasingly, providers have begun to make use of subcontractors by outsourcing functions that are not part of their businesses.

This situation can pose a threat to the company that is unaware of or has not provided for such a scenario, particularly since the company most likely will not have any contractual or other legal relationship with the subcontractor. Accordingly, at the negotiation stage with the service provider, the company should raise this issue and

include adequate provisions in any final contract to address its ability to obtain SAS 70 reports, as well as provide for other remedies vis-à-vis the service provider, to ensure that the financial reporting and internal controls of subcontractors are conducted in a way so as to comply with the company's Sarbanes-Oxley obligations.

In the relatively short time since its passage, the Sarbanes-Oxley Act has had a profound impact on corporate America. As various parts of the law have come into force, public companies have had to alter their business practices, including those affecting outsourcing operations, to comply with its provisions. With the PCAOB and the SEC having given some guidance regarding §404 of SOX, a particularly important provision of the act applicable to outsourcing, public companies will not only need to pay close attention to their outsourcing transactions at the negotiation and contract stages, but also will need to maintain sufficient authority over their service provider's internal financial control mechanisms to ensure compliance with the obligations that §404 imposes upon them.



1. The act does not apply to private companies. A timeline of the Sarbanes-Oxley Act's requirements can be viewed at [http://www.pwcglobal.com/Extweb/NewCoAtWork.nsf/docid/D0D7F79003C6D64485256CF30074D66C/\\$FILE/Timeline_Stand_Alone_Final_2.pdf](http://www.pwcglobal.com/Extweb/NewCoAtWork.nsf/docid/D0D7F79003C6D64485256CF30074D66C/$FILE/Timeline_Stand_Alone_Final_2.pdf) (last visited March 1, 2005).

2. The SEC final rules governing SOX can be viewed at <http://www.cfodirect.com/cfopublic.nsf?opendatabase&content=http://www.cfodirect.com/cfopublic.nsf/vContent/M/SRA-5QJQ6C?open> (last visited March 1, 2005).

3. See the PCAOB's Auditing Standard No. 2, which can be viewed at www.pcaobus.org/Rules_of_the_Board/Documents/Rules_of_the_Board/Auditing_Standard_2.pdf. p. 238 (last visited March 1, 2005).

4. Id.

5. Id.

6. See Management's Report on Internal Control Over Financial Reporting and Disclosure in Exchange Act Period Reports: Frequently Asked Questions, Securities and Exchange Commission, Office of the Chief Accountant and the Division of Corporation Finance, June 22, 2004, available at <http://www.sec.gov/info/accountants/controlfaq1004.htm> (last visited March 1, 2005).

7. See note 3, supra.

8. See Staff Questions and Answers, Auditing Internal Control Over Financial Reporting (June 23, 2004) available at www.pcaobus.org/Standards/Staff_Questions_and_Answers/Auditing_Internal_Control_over_Financial_Reporting_2004-06-23.pdf (last visited March 1, 2005).

9. See note 6, supra.

10. The issues raised here are not exhaustive, but rather are merely representative of some of the questions raised in the context of SAS audits and outsourcing.

This article is reprinted with permission from the March 8, 2005 edition of the NEW YORK LAW JOURNAL. © 2005 ALM Properties, Inc. All rights reserved. Further duplication without permission is prohibited. For information, contact ALM, Reprint Department at 800-888-8300 x6111. #070-03-05-0009