INTERNAL CONTROL REQUIREMENTS UNDER SARBANES-OXLEY
CHALLENGE OUTSOURCING MARKETPLACE

INTRODUCTION

In July 2002, amid public outcry over corporate accounting scandals and with the goal of restoring investor confidence, Congress passed the Sarbanes-Oxley Act of 2002 (the Act). The Act imposed significant new responsibilities on public companies, including a requirement that CEOs and CFOs certify that all quarterly and annual reports filed with the SEC fairly present the company’s financial condition.\(^1\) Related to the financial reporting certification is a requirement that management evaluate and report on the effectiveness of the company’s internal control over financial reporting. As public companies race to meet applicable compliance deadlines,\(^2\) businesses that have outsourced material portions of their information technology functions or important business processes are struggling to determine how to meet the Act’s requirement to assess control over financial reporting when a third party service provider performs processes that are a necessary part of such an assessment. This struggle has led to significant consternation and debate within the outsourcing marketplace over the role service providers should play in the customers’ efforts to meet the requirements of the Act. Specifically at issue is how much risk, if any, a service provider should bear in cases where the service provider’s controls impact the ability of its customers to satisfy the Act’s internal control requirements.

---

1 Executives who willfully certify false results face fines of as much as $5 million and as many as 20 years in prison. Also, companies that do not comply with the new rules risk being de-listed from stock exchanges.

2 The SEC recently extended the dates for companies to comply with the requirements of Section 404 of the Act. The SEC announced on February 4, 2004 that companies that are “accelerated filers” (those with a market capitalization of $75 million or greater) will not have to document their internal financial reporting controls and attest to the effectiveness of the procedures until their first fiscal year that ends on or after November 15. The original deadline for Section 404 compliance had been for fiscal years that ended on June 15 or later. In other words, companies with fiscal years ending on June 30 or September 30 have effectively been given one-year extensions of their compliance efforts, but the SEC’s extension does not afford companies that operate on a calendar year basis any additional time to comply. Companies that are not accelerated filers must begin to comply in fiscal years that end on or after July 15, 2005 – the original deadline had been April 15, 2004. See, http://www.alston.com/articles/Special%20Alert%202-26-04.pdf.
INTERNAL CONTROL REQUIREMENTS

Management’s Assessment

Section 404(a) of the Act and the related rules adopted by the SEC require management to assess the effectiveness of the company’s internal control over financial reporting as of the end of the company’s most recent fiscal year, and to state in the company’s annual report whether the company’s internal control over financial reporting is effective. The SEC rules implementing Section 404 of the Act include the following within the areas that management must consider in its assessment:

1. Controls over initiating, recording, processing and reconciling account balances, classes of transactions and disclosure, and related assertions included in the financial statements;

2. Controls related to the initiation and processing of non-routine and non-systematic transactions;

3. Controls related to the selection and application of appropriate accounting policies; and

4. Controls related to the prevention, identification and detection of fraud.

The rules require that the assessment be based on procedures sufficient to evaluate the design of the controls and to test their operating effectiveness, and that the assessment be supported by “evidential matter,” including documentation, regarding both the design of the controls and the testing process. Management must disclose any “material weaknesses” in its report and must state that internal control over financial reporting is not effective if there are one or more material weaknesses.3

Auditor’s Evaluation

Under Section 404(b) of the Act, the company’s independent auditor is required to evaluate management’s assessment process to determine whether management has an appropriate basis for reaching its conclusion concerning internal control over financial reporting. The Act calls for the creation of the Public Company Accounting Oversight Board (the PCAOB) to oversee the audit of public companies and, among other things, to adopt the standards relating to the preparation of audit reports, including the standards applicable to the attestations regarding internal controls. The PCAOB recently adopted

its Auditing Standard No. 2, which establishes the professional standards governing the independent auditor’s attestation and reporting on management’s assessment of the effectiveness of internal control over financial reporting, which the PCAOB concluded may only be conducted in conjunction with an audit of financial statements. Under Auditing Standard No. 2, the auditor would be required to both evaluate management’s assessment process and independently test the effectiveness of the company’s internal control to be satisfied that management’s conclusion is correct.

The auditor must render two opinions in its report: whether management’s assessment was “fairly stated, in all material respects”; and whether the company “maintained, in all material respects, effective internal control over financial reporting.” If the auditor concludes that internal controls were ineffective, the auditor’s report would also disclose any material weaknesses that led to its conclusion.

**IMPLICATIONS FOR THE OUTSOURCING MARKETPLACE**

A company’s decision to outsource functions to a third-party service provider does not reduce management’s responsibility under the Act to maintain effective internal control over financial reporting. Rather, for purposes of the company’s Section 404 obligations, to the extent the service provider’s services affect the company’s internal control over its financial reporting, management of the company and its auditors must consider the activities of the service provider in making their respective assessments. In its consideration, the company must (1) obtain an understanding of the controls at the service provider that are relevant to the company’s internal control over its financial reporting, as well as the control of the company over the activities of the service provider; and (2) obtain evidence that such controls are operating effectively.

---


5 The analysis contained in this portion of this advisory is based in part upon the guidance provided in the PCAOB Auditing Standard No. 2. As stated in footnote 4 of this advisory, Auditing Standard No. 2 has not been approved by the SEC and is therefore subject to change before it becomes effective. Readers are advised to monitor developments with regard to Auditing Standard No. 2.
Understanding Relevant Controls

It is not always evident when the functions performed by a service provider form a part of the customer’s internal control over its financial reporting. Transactions that by their nature involve a customer’s financial reporting include certain business process out-sourcings (such as finance and account processing, loan processing or HR processing) where management of the financial documentation is usually a component of the service provider’s obligations, or where a service provider may be given authority to make decisions over processes that affect the customer’s financial reporting. Less obvious are IT infrastructure and data processing transactions. IT often enables the controls sought for reliable financial reporting in areas such as information management, data classification, real-time reporting, and data transmission and validation. In such cases, the service provider’s controls do affect the customer’s financial reporting and are relevant to the customer’s evaluation of its internal controls. In addition, where service providers process data utilized in creating the company’s financial statements, management must assess the service provider’s general computer hardware controls, application change controls, controls that restrict access to programs and data, and controls that affect the processing of data.

Evidence of Effectiveness of Service Provider Controls

Once company management or the company’s auditors have determined the relevant service provider controls that form a part of the company’s internal control over its financial reporting, management must obtain evidence that such controls are effective. Such evidence may be obtained by one or more of the following: (1) performance by the company or its auditors of tests of the company’s controls over the service provider (i.e., testing that the company’s processes provide adequate controls over the service provider’s activities, independent of the service provider’s controls); (2) performance by the company or its auditors of tests of the relevant service provider controls; or (3) obtaining a report of the service provider’s auditor that the relevant service provider controls are effective for purposes of the company’s financial reporting. In each case,

---

6 In addition to the SEC rules implementing Section 404, which apply generally, PCAOB Auditing Standard No. 2 directs companies to the American Institute of Certified Public Accountants (AICPA) Professional Standards (AU) sec. 324 which states that a service provider’s services are part of a company’s information system, and therefore applicable to an audit of the company’s financial statements, if the services affect any of the following:

- The classes of transactions in the company’s operations that are significant to the company’s financial statements;
- How a company’s transactions are initiated, recorded, processed and reported from their occurrence to their inclusion in the financial statements;
- The accounting records, supporting information and specific accounts in the company’s financial statements involved in initiating, 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; or
- The financial reporting process used to prepare the company’s financial statements.
determining whether the relevant service provider controls are effective must be included as part of the company’s assessment of whether its internal controls are effective for purposes of the company’s Section 404 obligations.

DEAL IMPACTS

In outsourced environments where control over a company’s financial reporting is affected by services performed by the service provider, the customer faces several issues:

1. How can the customer monitor and assess the relevant service provider controls to ensure that they operate effectively such that the customer can meet its obligations under the Act? How can the customer require changes to the relevant service provider controls if they are found not to be effective?

2. What risk and liability should the service provider incur in connection with the customer’s obligations to comply with its internal control requirements under Section 404?

We expect that customers will seek to address these issues in the context of their outsourcing deals and the related contractual terms.

Monitoring

Since the company retains responsibility for ensuring adequate internal control over its financial reporting, it must have the necessary contractual rights in its outsourcing agreement to require that the relevant service provider controls operate effectively. Sufficient due diligence can be conducted at the beginning of the outsourcing arrangement to confirm that the initial processes and procedures are in place to meet this requirement. However, as the contracted services change and as the processes and procedures used to perform the services change, the controls (on both sides) may be required to change as well. As discussed below, the issue is which party should bear the risk (i.e., the cost of compliance) when either party’s controls must change to accommodate changes in the services.

Company Audits

Assuming that the necessary controls are initially in place for management to make its assessment, the company must continue to monitor the relevant service provider controls. Such monitoring can be done through contractual audit rights retained by the customer. General audit provisions in outsourcing agreements provide companies the right to audit various aspects of the service provider to ensure that the service provider is performing the services in accordance with its contractual obligations. Such audits can be used to test the effectiveness of the relevant service provider controls, and accordingly can be used as evidence as to the effectiveness of such controls. These
general audit provisions usually have restrictions, however, as to scope, frequency and timing.

**SAS 70 Reviews**

Where companies and their auditors do not directly test the relevant service provider controls, companies and their auditors may rely in part upon SAS 70 reports prepared by the service provider’s auditor for evidence that the service provider controls are effective. The AICPA prepared SAS 70 to provide guidance to auditors of service providers on their reporting on a service provider’s controls that may affect a company’s internal controls over financial reporting. SAS 70 reports come in two types: Type I (which describes the service provider’s controls at a specific point in time); and Type II (which contains the Type I information and also describes detailed testing of the service provider’s controls over a minimum six-month period). While a company and its auditors cannot rely solely upon a SAS 70 Type II report to meet their respective obligations under Section 404 of the Act, such reports can be used as evidence that the relevant service provider controls are effective for purposes of the company meeting its assessment and certification obligations under the Act, and for the company’s outside auditor to render its required opinion. The PCAOB directs companies and auditors that elect to use SAS 70 reviews to independently evaluate whether the report provides sufficient evidence to support management’s assessment or the auditor’s opinion.

In many instances large service providers conduct SAS 70 reviews on a regular basis (often annually) and make the resulting reports available to their customers. In some instances those reviews are tailored specifically to the needs of the company. In many instances, however, particularly in IT outsourcing arrangements where services are provided out of shared data centers, the SAS 70 contemplates only a review of the service provider’s internal controls generally and not as specifically related to the controls of its customer base. Given the heightened customer interest in service provider control environments resulting from the Act, it is not surprising that issues related to SAS 70s have recently taken a high profile in outsourcing negotiations. Specifically, a debate has taken shape as to what degree service providers should be responsible for SAS 70 reviews in a shared environment that contemplate the specific scope requirements.

---

7 American Institute of Certified Public Accountants’ (AICPA) Statement on Auditing Standards (SAS) No. 70, Reports on the Processing of Transactions by Service Organizations.

8 SAS 70 Type I reports cannot be used as evidence that the relevant service provider controls are effective because they do not test the effectiveness of the relevant service provider controls.

9 See paragraph .21 of AICPA Professional Standards (AU) sec. 324 that states: “The [company] auditor should not make reference to the report of the service [provider] auditor as a basis, in part, for his or her own opinion on the [company]’s financial statements. The service [provider]’s auditor’s report is used in the audit, but the service [provider] auditor is not responsible for examining any portion of the financial statements....”

10 According to PCAOB Auditing Standard No. 2, such evaluation should be based upon the time period covered by the test of controls, the scope of the examination and the applications covered, the controls tested, the results of those tests, and the competence and objectivity of the service provider auditor performing the test.
of individual customers and their particular financial reporting issues. For example, should the scope of the service provider’s SAS 70 report cover all controls that impact all of its customers’ financial statements? Likewise, should the effective date of the SAS 70 report sync with all of their customers’ annual reporting requirements? If not, the timing of the service provider’s SAS 70 report may be such that the company cannot use it for its own assessment purposes. One solution to the timing issue proposed by company advocates is that service providers be required to conduct multiple SAS 70 reviews each year, which would always provide at least one recent report for the company to use for purposes of its annual assessment regardless of its fiscal year-end.

These and similar issues have left the customer community and the service provider community at odds over which party should be responsible for the increased costs associated with more frequent or customized SAS 70s. Service providers have generally been loathe to allow customers in a shared environment to have any control over the scope or timing of their SAS 70 reviews, stating that they cannot reasonably meet the requirements of all of their customers in a shared environment. Accordingly, the service providers argue that they must create a generic report that seeks to meet the general needs of the majority of their customers, and not the specific needs of any one. Customers, on the other hand, argue that generic SAS 70 reviews conducted by service providers are of limited use to customers if they have no control over scope and timing. CEOs and CFOs have been calling upon service providers to view the SAS 70 review process as an opportunity for them to differentiate themselves in the marketplace while helping their customers to meet their statutory obligations under the Act. Most service providers have not yet seized upon that call.

**Other Affected Contract Terms**

In addition to increased focus on audit rights, it is likely that customers will seek greater contractual control over service delivery related to functions that affect the customer’s financial reporting. For example, customers may tighten restrictions on the right of service providers to subcontract the performance of functions that directly affect the customer’s financial reporting. In addition, customers may obligate service providers to obtain SAS 70 reports from subcontractors where necessary to allow the customer to meet its obligations under Section 404. Customers may also seek more control over the procedures used by service providers to perform functions that affect the customers’ financial reporting. Processes and procedures typically left to the discretion of service providers may become the subject of greater customer scrutiny and control through more robust statements of work, procedures manuals and reporting requirements. Lastly, customers may seek to augment account governance structures with resources dedicated to monitoring and assessing relevant aspects of the service provider’s controls. In many instances, these more stringent terms will drive costs into outsourcing transactions, and the allocation of such costs will need to be agreed upon.
RISKS AND LIABILITIES

Allocation of Compliance Costs

Many companies have complained about the cost of complying with Section 404 of the Act. Where an outsourcing arrangement is introduced into the equation, thereby increasing compliance costs, customers have argued that service providers should share some of the incremental costs of compliance. In addition to the costs related to SAS 70s discussed above, cost issues arise when a party to the outsourcing agreement must change its control environment to accommodate either changes in the other party’s control environment or changes in the services provided. In these cases, the parties must agree upon a fair allocation of costs commensurate with pricing under the agreement and the associated risks.11

Allocation of Risks

While service providers have no direct compliance obligations under the Act with respect to their customers’ Section 404 obligations, customers have argued that the risk of non-compliance (and associated liability) should be shared with service providers when deficiencies in the service provider’s controls prevent the customer from making an affirmative statement as to the effectiveness of its internal controls.12 Any shifting of risk and liability to the service provider would have to be negotiated in the outsourcing contract.

As stated above, one method of shifting risk is for the contract to include a provision that requires the relevant service provider controls to be effective for purposes of the company meeting its obligations under the Act. Failure to meet that contractual requirement would result in a breach of the agreement that would presumably provide the company some remedy. Another contractual provision that could be included in the outsourcing contract is a certification on the part of the service provider that the service provider’s controls are effective such that the management of the company can make its assessment under Section 404.13 However, service providers are highly reluctant to provide such certifications, representations or other contractual assurances so as to avoid any additional liability that might attach to their breach. If a service provider did provide such contractual assurances, it would likely protect itself by limiting the

---

11 One view is that compliance with Section 404 should not be treated differently than other compliance with laws provisions under outsourcing agreements. Often in those agreements, the party necessitating the change bears the cost of compliance, and in instances when the change results from statutory or regulatory changes, the parties agree upon a cost-allocation mechanism.

12 We note that the company can only shift financial, and not criminal, penalties.

13 Even if a service provider is willing to make such a certification, the PCAOB Auditing Standard No. 2 does not allow the company or its auditor to rely on the certification as a basis for fulfilling their respective obligations under Section 404.
amount of its liability and requiring the customer to waive any right to indirect or consequential damages. Even if companies are able to include such contractual provisions in their outsourcing contracts, a service provider will seek to charge higher prices for any increased associated risks it perceives. With or without contractual assurances from the service provider, the company must conduct (through its independent auditor) its own evaluation of the service provider’s activities that are a part of the company’s financial reporting, and accordingly the contractual provision would primarily serve to limit the company’s financial exposure in the event that the service provider’s controls are inadequate. When taking into account the increased pricing and restrictions and allowable remedies, companies should consider whether they will receive sufficient value for the introduction of such contractual provisions. Inclusion of such provisions could be deemed part of a company’s control over its financial reporting, and for that reason, such provisions may have independent value.

A COLLABORATIVE APPROACH

As the deadline approaches for companies to fulfill their Section 404 requirements, the debate continues to intensify over the extent to which service providers should share in customers’ responsibilities. The time may be ripe for the industry to take a collaborative approach to addressing the issue. Service providers, customers and accounting firms might be well served by collectively and proactively addressing the issue and formulating uniform approaches. For example, the scope of SAS 70 reports in the context of a shared data center could be standardized, or standard contractual provisions that address compliance with internal control requirements could be crafted. It remains to be seen whether solutions to the unique challenges posed by Section 404 will be solved collectively within the outsourcing marketplace. In the meantime, parties to outsourcing agreements will be forced to reach their own resolutions on the myriad of issues described above.
This Outsourcing Advisory is published by Alston & Bird to provide a summary of significant developments to our clients and friends. It is intended to be informational and does not constitute legal advice regarding any specific situation. This material may also be considered advertising under the applicable court rules. If you have any questions or would like additional information, please contact the authors, any member of the Alston & Bird Outsourcing Group or your Alston & Bird attorney.

This advisory prepared by:

David E. Brown, Jr.  
202-756-3345  
dbrown@alston.com

Christopher D. Ford  
202-756-3371  
cford@alston.com

Karen M. Sanzaro  
404-881-7275  
ksanzaro@alston.com

James J. Casey  
202-756-3332  
jccasey@alston.com

Catherine A. Meeker  
704-444-1077  
cmeeker@alston.com

Scott W. Stevenson  
202-756-5580  
sstevenson@alston.com

MEMBERS OF ALSTON & BIRD’S OUTSOURCING GROUP

Shawn K. Baldwin  
404-881-7914

Lisa K. Hoskin  
404-881-4784  
britton@alston.com

Britton T. Richardson  
404-881-4828

Matthew S. Branson  
202-756-3395

David C. Keating  
404-881-7355  
keating@alston.com

Karen M. Sanzaro  
404-881-7275

Janine Brown  
404-881-7834

Jay S. Krutulis  
202-756-3348  
jkrutulis@alston.com

Scott W. Stevenson  
202-756-5580

James J. Casey  
202-756-3332

David L. Mathus  
212-210-9436  
mathus@alston.com

George M. Taulbee  
704-444-1023

Wayne H. Elowe  
404-881-7672

Todd S. McClelland  
404-881-4789  
mcclelland@alston.com

Angela Vitale  
202-756-5587

Christopher D. Ford  
202-756-3371

James E. Meadows  
404-881-7329

C. Chad Warpula  
704-444-1034

James A. Harvey  
404-881-7328

Robert C. Reynolds  
404-881-7560  
reynolds@alston.com

John C. Weitnauer  
404-881-7780

Darren C. Hauck  
404-881-7946

If you would like to receive future Outsourcing Advisories electronically, please forward your contact information including e-mail address to outsourcing.advisory@alston.com. Be sure to put “subscribe” in the subject line.