

## Negotiating in a Sarbanes-Oxley World

Richard Pennington, J.D., C.P.M., Consultant

SCOPEVision Consulting Ltd

303/324-7333, [rpennington@scopevisionconsulting.com](mailto:rpennington@scopevisionconsulting.com)

### 91<sup>st</sup> Annual International Supply Management Conference, May 2006

**Summary.** This paper provides a background on the Sarbanes-Oxley Act (SOX) and its impact on negotiations by supply management professionals. SOX does not dictate contract negotiation outcomes, but a basic understanding of SOX is important for planning negotiations and anticipating possible SOX issues. The essential steps of negotiation – planning, understanding the issues and needs of the other side, assembling the appropriate teams, formulating communication strategies and options – are implicated in new ways in the world of Sarbanes-Oxley. Even for nonprofit and governmental organizations not technically covered by the statute, SOX has resurrected visibility of internal controls in organizations. Organizations' interests that must be accommodated include integrity in financial reporting and a process for evaluating risk in transactions. The use of service organizations, those outsourced arrangements directly touching financial reporting in a material way, adds substantive issues to any complex negotiation.

**Background of Sarbanes-Oxley.** In 2002, after the financial reporting debacle created by the Enron and WorldCom failures, Congress passed the Sarbanes-Oxley Act of 2002 (SOX). SOX applies to publicly-traded companies and is aimed at creating an environment in which financial performance is reliably and accurately reported. Section 302 of the new statute placed on management a new responsibility to prepare certifications of financial statements of publicly traded companies. The statute created new expectations for boards in terms of their accountability for financial reporting, added financial expertise requirements to membership on boards, and has changed the relationship between companies and auditors. The statute created the Public Company Accounting Oversight Board (PCAOB) to set auditing standards.

Section 404, the central part of the legislation from an internal controls perspective, added a new requirement that senior management annually assess and report on the effectiveness of internal controls. Annually, auditors are required to attest to both the organization's assessment of effectiveness of internal controls and render an independent opinion about the effectiveness of internal controls. Previously, the internal controls of a company were considered in the overall context of a financial audit but not separately certified. Understandably, this emphasis has the effect of raising awareness about internal controls concepts and interjecting SOX concerns into operations, including supply management.

**The New Negotiation "Need": Visibly Effective Internal Controls.** Early commentators predicted that SOX would impact not only financial controls and reporting, but that certifications would target operational aspects of organizational performance as well.

The current internal controls model has been in use in the United States for 20 years, via the establishment of the Committee of Sponsoring Organizations of the Treadway Commission (COSO). The commission arose out of early concerns about integrity in financial reporting. In 1992, the COSO *Internal Controls – Integrated Framework* was issued.

“Internal controls” are broadly defined as a process that provides reasonable assurance regarding the achievement of organizational objectives: reliability and accuracy in the case of financial reporting. The COSO *Framework* embraces more than just financial reporting and extends to operations and statutory compliance. The COSO *Framework* is a conceptual model having multiple components: an organizational control environment, risk assessment, control activities, information and communications, and monitoring. Controls are generally divided into preventive controls (such as adequate training and segregation of duties between purchasing and accounts payable) and detective controls (like post transaction reconciliation of procurement card purchases and management reviews). In the case of financial reporting, the objective is to achieve a set of controls that provide “reasonable assurance” that statements are reliable and that misstatements and fraud will be prevented, deterred, or timely detected. Reliability means financial statements are fairly presented in material respects, in conformity with generally accepted or other relevant and appropriate accounting principles and regulatory requirements.

In its final rulemaking in August 2003, the SEC clarified that the SOX regulations encompassed only the subset of COSO internal controls that pertain to financial control objectives. The regulations do not include elements of the COSO definition that relate to effectiveness and efficiency of a company's operations. Consequently, the touchstone of the SOX internal controls review is on financial reporting. In short, this means that a company can have operational problems so long as it is making the proper disclosures in its financial reports. Of course, some operational issues can be so significant as to require disclosure in reports.

Widely held views about the costs of compliance were aired at the April 13, 2005 *Roundtable Discussion on Internal Control Reporting Provision* held by the SEC. The frustrations expressed about SOX implementation included: reluctance of auditors to use risk-based methods; perceived limitations on external auditors' use of internal auditor work; excessive conservatism and disagreements about “materiality” and “significance” of control deficiencies; the value of the amount of IT controls testing; use “one size fits all” or checklist approaches; and the chilling of relationships with auditors.

Much of the commentary today continues to emphasize the amount of spending on SOX internal controls and whether the investments – sometimes overwhelming in information technology – are offset by the benefits. But there have been anecdotal accounts of internal auditors appearing as members of contract negotiation teams, sometimes making representations about what Sarbanes-Oxley will and will not permit. Largely, the notion that SOX drives any particular negotiation result is a myth, although SOX has added new awareness about internal controls and additional visibility into companies' internal controls structures, including those that are impacted materially by outsourcing. And because sound auditing practices are further defined by auditors' professional associations (e.g. the American Institute of Certified Public Accountants), one can expect the evolving impact from these issues to migrate to any organization that undergoes audits of its financial statements -- private, public, or governmental.

**The Interests.** Any negotiation represents an attempt by both parties to achieve objectives that are better than the alternative to negotiated agreement. Volume 2 of the ISM Supply Management Knowledge Series outlines the essential steps in negotiations. Understanding

the issues and needs of each party are critical. SOX has changed the emphasis on and added to the range of organizational interests.

The primary purpose of SOX was to promote integrity in financial reporting. For companies having to report financial performance to the SEC, government regulators, investors, or others needing the financial information, this is achieved through the audit process. Ultimately this means that organizations want unqualified or “clean” opinions, requiring that they do an adequate job of internal controls management. Of the 14% of companies reporting material internal control deficiencies in 2005, the deficiencies involved issues that one would expect with financial reporting and potential fraud: income tax matters; revenue recognition; inventory; lease accounting; application of generally accepted accounting principles (GAAP) to liabilities; segregation of duties; and IT control, among others. Traditional contract issues, those often associated with procurement concepts of “risk,” were not among those reported. But because management has to conduct and certify independent reviews of internal controls, the internal auditor may play a different or greater role in transaction processing.

PCAOB Auditing Standard No. 2 contains only one example of an internal control deficiency in a purchasing context. Example D-2 describes a situation where standard shipping terms are modified by sales personnel without review by the accounting office, potentially leading to erroneous recognition of revenue. The problem is not that the terms are agreed to. It is that the accounting entries are not proper.

While SOX does not dictate how organizations manage contractual risk, some business judgments may be considered unreasonable, warranting disclosure in the mind of auditors. So while analysis of a business risk remains an organizational responsibility, there may be a tendency by some auditors to substitute their judgment if they believe risk is material and would have been of interest to potential investors or others who rely on financial statements. This is where the universe of the auditor may intersect that of the contract negotiator in transactions that are considered “material.” It is important during the negotiation to stay attuned to issues that involve this kind of sensitivity. It is also important to ally oneself with an internal auditor should these kinds of issues surface during contract negotiations.

**Plan Communication Strategies.** Of importance in any negotiation is identification of the information one needs from the other side, and being prepared to “fact find” in a dynamic environment. Internal controls issues may blur the common understanding that supply management professionals have of terms used during negotiation. Plan ways to identify the interests relating to internal controls and probe gently for underlying motivations as unexpected internal controls or “risk” issues are introduced during negotiations.

For example, the concept of “risk assessment” is one area that needs clarification if the term is raised in negotiations. Once that term is used, especially where internal controls or SOX is implicated, get clarification. In a financial reporting context, the term is defined this way in PCAOB Audit Standard No. 2:

The auditor should evaluate whether management has identified the risks of material misstatement in the significant accounts and disclosures and related assertions of the financial statements and has implemented controls to prevent or detect errors or fraud that could

result in material misstatements. . . . the risk assessment process should address how management considers the possibility of unrecorded transactions or identifies and analyzes significant estimates recorded in the financial statements.

Purchasing professionals commonly discuss risk in a different way, such as liability limitation, liability and risk allocation, and indemnification. Confusion about the varying definitions of “risk” has been acknowledged by COSO and largely led to its 2001 enterprise risk management project. It helps to know that the focus of “risk” in the SOX context is on financial reporting: not accounting for all transactions; alterations of transactions; erroneous application of accounting rules; improperly recording entries, e.g. to the wrong period or in the wrong amount; misappropriation of assets; or recording transactions that did not occur.

Consequently, in any negotiation where “risk” becomes one of the criteria for agreement, reach a clear understanding about what is being discussed. Otherwise, one loses the ability to respond at the bargaining table. SOX does not permit or prohibit a company’s agreeing to anything. SOX requires only that an organization’s internal controls include processes to consider and evaluate risk, and that appropriate financial entries are made.

Internal control processes implicate another common issue in negotiation -- time. Time often can be a source of power by one party. As emphasis on internal controls increases, one can expect more attention to be paid to internal approvals. The size and frequency of a transaction relates to “materiality” and “significance” in internal controls, an acknowledgment that risk changes with value. Know what the approval requirements are by asking about the approval steps and the persons who must be involved. Ideally, get those persons to the negotiating table if time is of the essence. One can expect the number of persons involved in and the time for negotiation to increase in this new era of internal controls awareness.

**Planning for Possible Options.** Negotiation planning includes identification of a range of potential options on important issues, from the optimal result to one your company “can live with.” Forecast the other party’s probable options as well.

Companies manage risk often by establishing standard terms and conditions in contracts. While SOX does not dictate negotiation results, it is placing greater emphasis on processes -- identifying and evaluating deviations from standard practice. Ask for the other party’s standard contract terms as a way of anticipating potential issues. For example, Auditing Standard No. 2 lists deviation from standard payment/delivery terms as a source of risk. Similarly, expect to have to plan more for negotiations that involve rebates and revenue recognition issues from creative financing provisions; warranties, performance guarantees and hardware/system service level agreements (SLAs); risk of loss clauses; and other liability allocation provisions such as limitations of liability and indemnification.

While SOX does not dictate any particular approach to these issues, one can expect to encounter greater involvement by senior management with these issues in large transactions or even routine ones that deviate from a company’s – yours or the other party’s -- standard terms.

**An Issue Having New Importance: Outsourced Financial Operations -- Service Organizations.** In the case of outsourced operations where those activities are part of the client (using) organization's financial reporting "information system," those outsourced companies – known as "service organizations" – could be considered part of the internal controls structure of the using company. Then any audit of internal controls would extend to the controls of the service organization. Not all outsourced activities are part of this information system. The arrangements of interest are those in which a client agency's significant transactions are initiated, authorized, recorded, processed, and reported from their incurrence to their inclusion in the financial statements. In that event, those activities would be subject to internal controls review and audit. A statement of work in such an agreement – or a modification to an existing agreement -- would have to define expectations, many of which involve significant costs.

The PCAOB emphasizes a "top-down" approach in internal controls auditing, reinforcing the conclusion that there is no single, objective answer to questions about what processes and procedures must exist in any internal control environment, including outsourced financial operations. The COSO evaluation matrices for internal controls likewise are described as "illustrative," requiring tailoring by companies. To an auditor, the company's existing control environments serve as a roadmap to understanding what is significant in the context of the company's business. Consequently internal auditors and other personnel central to the control environment will have to be involved in negotiation planning where service organizations internal control systems are involved. The lesson: involve your own auditors in planning for any contract negotiation that involves outsourcing of key business processes.

Requiring audits or cooperation by contractors is not a right that exists independent of a contract. A procurement or subcontract management office in many cases would have to consider provisions relating to:

- Expectations about assistance the using organization requires to understand the service organization's internal controls
- Provision of and/or access to documentation, e.g. manuals, necessary to show effectiveness of internal controls
- Records retention requirements
- Service organization responsibility relative to testing of its controls or participating in user organization tests of controls
- Access to employees for "walkthroughs" and testing of controls
- The obligation to provide such additional documentation or cooperation as is required to satisfy the using company's auditors
- Responsibility for providing a service auditor's report (e.g. SAS 70 Type II report) on controls placed in operation and tests of operating effectiveness or a report after use of agreed-upon procedures that describes relevant tests of controls; define timing and scope of the report as well as qualifications/identity of the auditor providing the opinion

While a user company can rely on service auditor reports in some cases, the expectations have to be defined contractually. In some cases, where there are existing contracts, provisions need to be renegotiated that provide a suitable report or permission to test controls at the service organizations. Otherwise, the using company may face an adverse or qualified

opinion. The using company's internal audit function has to be part of the negotiation planning in order to identify the outsourcing arrangements that would be of interest and adequately define the expectations for the service organization.

**Conclusion.** Even though the technical SOX requirements apply only to publicly traded companies, one can expect the focus on internal controls to migrate across all organizations that have their financial statements audited. Even apart from procurement operations, these issues may work their way into contract negotiations as auditors further define expectations for internal controls. Especially in outsourcing situations, these interests will have to be integrated by purchasing professionals into negotiation planning. Involve your own company's internal auditing function.

## REFERENCES

The Committee of Sponsoring Organizations of the Treadway Commission, *Internal Control – Integrated Framework Guidance for Smaller Public Companies Reporting on Internal Control over Financial Reporting (Draft)*, <http://www.ic.coso.org>, October 2005.

Deloitte & Touche LLP, Ernst & Young LLP, KPMG LLP, Pricewaterhouse Coopers LLP, *Perspectives on Internal Control Reporting*, December 2004.

Fawcett, Stanley, *The Supply Management Environment*, Institute of Supply Management, Inc., Tempe AZ, 2000.

Moeller, Robert, *Sarbanes-Oxley and the New Internal Auditing Rules*, John Wiley & Sons, Inc., Hoboken NJ, 2004.

Public Company Accounting Oversight Board, *Auditing Standard No. 2: An Audit of Internal Control Over Financial Reporting Performed in Conjunction with An Audit of Financial Statements*, [http://www.pcaobus.org/Rules/Rules\\_of\\_the\\_Board/Auditing\\_Standard\\_2.pdf](http://www.pcaobus.org/Rules/Rules_of_the_Board/Auditing_Standard_2.pdf), March 9, 2004.

Public Company Accounting Oversight Board, *Roundtable Discussion on Implementation of Internal Control Reporting Provisions*, <http://www.sec.gov/spotlight/soxcomp/soxcomp-trans.txt>, April 13, 2005.

PCAOB Release 2005-009, Policy Statement Regarding Implementation Of Auditing Standard No. 2, PCAOB Release No. 2005-009, [http://www.pcaobus.org/Rules/Docket\\_008/2005-05-16\\_Release\\_2005-009.pdf](http://www.pcaobus.org/Rules/Docket_008/2005-05-16_Release_2005-009.pdf), May 16, 2005.

Securities and Exchange Commission, *Final Rule: Management's Reports on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports*, <http://www.sec.gov/rules/final/33-8238.htm>, June 5, 2003.