

March 2006

Sarbanes-Oxley Basics for Risk Managers - Controls for TPA Services

Since 2002, Sarbanes-Oxley compliance activities have been center stage for large public companies. Risk managers play an important role in applying these requirements to TPAs. The controls go far beyond the usual claim file audits, and the payoff is beyond sheer compliance. This process will benefit your organization by improving claim performance and data quality and by confirming that your TPA is delivering on contractual promises. Audit results are particularly useful when you change TPAs and want to monitor differences in reserving and payment patterns.

What is Sarbanes-Oxley?

Passed by Congress in 2002 as a result of high-profile business scandals, including the bankruptcies of Enron and WorldCom, the Sarbanes-Oxley Act establishes many new requirements for public companies' managers and independent auditors. In effect, it requires that public company managements be confident – and certify to the SEC – that their financial statements are accurate and complete; and further, that the company's processes and procedures for assuring accurate financial reporting are both sound and operating properly. The company's independent auditors must not only certify the company's annual financial statements, but also attest to the quality and completeness of management's report on internal financial controls.

Risk Management Audit of TPA Services

When outside service organizations are responsible for "significant"¹ financial transactions on behalf of the company, company management must determine whether both internal controls and the service organization's controls are adequate to assure accurate financial reporting.

Risk managers employ third party claims administrators (TPAs) for their flexibility, professionalism and cost effectiveness. In particular, alternative risk financing options, including self-insurance, large deductibles, captives, retrospective and association programs, often use TPAs.

Because a TPA makes claim payments on behalf of its clients, risk management departments must assess and monitor the financial controls in place both internally and

at the TPA for accurate claim payments, fees, discounts, and other charges and credits. The amount of payment activity compared to TPA fees varies with the line of business, but often a TPA is processing payments twenty times greater than its fees.

There are five key steps involved in a TPA financial controls audit:

1. Review TPA contracts, special account instructions, written "best practices" and all other relevant documents, and list all elements relating to specific performance measurements, fees, discounts, payment handling, invoicing and controls.
2. Obtain a SAS 70 Type II² service auditor's report from the TPA, evaluate for completeness, and note any deficiencies in key controls involving the services provided to the company.
3. Perform tests of controls at the TPA site(s). At a minimum, discrepancies identified in the SAS 70 should be retested; if the TPA's SAS 70 Type II is out of date, qualified by the auditor or nonexistent, then direct testing of controls at the TPA needs to be much broader in scope.



RIMSTech Bulletins are published periodically by the Technology Advisory Council (TAC) to outline technology issues of interest to risk managers. They are not intended to endorse specific products or services. RIMS provides the information in these bulletins as a benefit and service to its members. RIMS makes no representations about the accuracy or suitability of the information for any purposes.

THIS ISSUE'S CONTRIBUTOR

Fred Travis is a Senior Associate Consultant with Shelter Island Risk Services; he spent more than twelve years as Director, Corporate Safety & Risk Management for Anheuser Busch Companies, Inc. He can be reached at (636) 742-2256 or FWTravis@sirisk.com.

CONTACT TAC

If you have an idea for a RIMSTech Bulletin or have comments you want to share, contact by e-mail any of the following individuals:

- **Jeff Stolle**, TAC Chair and RIMSTech Advisory Board, jeff.stolle@pepsico.com
- **Patty Born**, RIMSTech Advisory Board, patricia.born@csun.edu
- **Bob Henderson**, RIMSTech Advisory Board, robert.j.henderson@marsh.com
- **Angus Rhodes**, RIMSTech Advisory Board, angus.rhodes@aon.co.uk
- **Michael Scott**, RIMSTech Advisory Board, michael_scott@admworld.com
- **Meg McGeady**, RIMS, mmcgeady@rims.org

Known transaction errors identified by the company in the previous 12 months should also receive scrutiny. Special attention must be devoted to manual processes, including claim intake and coding bills to specific clients and claims, to be sure errors are found and corrected systematically.

4. Assess the design of company internal financial controls over the TPA's transactions ("user controls"). This is particularly important where the TPA's controls are found to be flawed or inadequate.
5. Test internal financial controls. As in #3 above, particular attention should be directed to manual processes.

Auditing financial controls involves examining both design and testing issues. Design issues include such elements as:

- Alignment between the control and the business risks identified. For example, does an input system for medical bills automatically prevent duplicates from being entered?
- Frequency with which the controls are applied. Will the controls detect or prevent the risks identified on a timely basis?
- Knowledge and experience of the people involved in performing control activities.
- Segregation of duties relevant to the process being controlled.
- Processes and procedures to address exceptions that result from the control activity.
- Reliability of the information used in the performance of the control.

Testing issues include standard accounting and statistical elements, including determining sample size, creating test data, developing test plans and procedures, and identifying and classifying exceptions.

Controls found to be inadequate must be categorized as "deficient," "significantly deficient," or exhibiting a "material weakness," depending upon the seriousness of the deficiency and the sums at risk relative to the overall impact on the company. Deficient controls must be redesigned, installed and retested often until they prove effective.

Ongoing Monitoring of TPA and User Controls

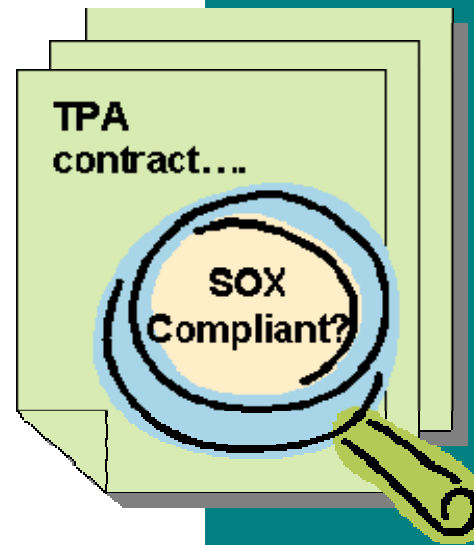
To assure continuing credibility of financial controls, risk management departments should adopt plans and procedures to periodically test all controls identified through an initial audit. Some examples of continuous monitoring include:

- **Input/Output comparison** – Transaction information provided by the company to the TPA (such as social security numbers of claimants) should be compared to the information in the TPA's system on a regular basis, so keying errors may be found and corrected.
- **Performance indicators** – All specific performance measures specified in contracts, special instructions and written "best practices" should be checked for compliance quarterly, or as often as necessary, to assure timely corrective action. This will require reconciliation of payment transactions and claim records to insure the accuracy of loss runs provided for financial and actuarial applications.
- **Process controls** – User controls should be set up to review and reconcile TPA invoices and analyze discounts, fees, and special charges so that all such charges may be compared to contractual requirements (for example, medical re-pricing savings), screened for duplicates and confirmed as correct.
- **Fraud detection** – Periodic analysis of large payees, identification of "repeat" claimants and other measures necessary to uncover improper payments.

Conclusion

The Sarbanes-Oxley Act affects large public companies and all of their important operations. Because of the specialized risks and systems involved with TPAs, risk management departments should take a lead role in assessing controls and setting up ongoing monitoring. Risk management departments are much more knowledgeable about TPA processes than internal or independent auditors and can apply their expertise to produce superior results.

A TPA has significant authority and responsibility for making payments on behalf of its clients. You can generally assume that for each \$50,000 in fees you pay a TPA; the TPA dispenses \$1,000,000 on your behalf. For this reason, the controls described here are not a 'nice to have' but a 'must-have' requirement.



Footnotes:

1. "Significant" is not defined in the Sarbanes-Oxley Act, but generally means an amount, whether as a single transaction or in the aggregate, that if incorrect would potentially cause the company's financial statements to be incorrect. As a rule of thumb, \$1,000,000 would generally be considered "significant" for a Fortune 1000 company.
2. A SAS 70 Type II report summarizes an outside auditor's assessment of both the design and the operation of a service organization's process controls. To be useful, the report must cover the processes and controls that are relevant to the service organizations clients.

TAC welcomes feedback on this bulletin and suggestions of topics for future bulletins. Topics and content are the sole discretion of TAC.