



White Paper Series

Issue No. 001
April 2006

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

This White Paper is a publication of Shelter Island Risk Services, a subsidiary of Gallagher Bassett Services, Inc. The White Paper series is designed to examine current and emerging issues that impact the field of Risk Management. For more information about Shelter Island, and to access our archive of past publications, please visit www.shelterislandrisk.com.

Fred Travis
Shelter Island Risk Services
636.742.2256
fwtravis@sirisk.com

Richard F. Denning
Shelter Island Risk Services
631.749.1535
rfdenning@sirisk.com

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 third-party claim administrators (TPA's). The controls suggested here 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. The process is particularly useful when you change TPA's and want to monitor differences in reserving and payment patterns.

Some Risk Managers think of Sarbanes-Oxley as someone else's problem. Think again! The self-assessment below should make it clear that Risk Managers have a direct Sarbanes-Oxley responsibility because, as bank robber Willy Sutton famously said, "that's where the money is". A TPA has significant authority and responsibility for making payments on behalf of its clients. As a rule of thumb, for each \$50,000 in service fees you pay a TPA, the TPA pays out \$1,000,000 on your behalf. Consider. . .

1. Does your TPA provide you with a current SAS70 Type II report? If you're not familiar with this document, footnote #2 below is a brief explanation.
2. Do you reconcile TPA payments and fees "as billed" to TPA payments "as reported" and actual services performed in your claim data system on a monthly/quarterly basis?
3. Have you or your internal audit department already performed a Sarbanes-Oxley controls audit of your program? Were the results satisfactory?
4. Do you have systematic processes and procedures for identifying and correcting TPA data and transaction errors?

IF YOU ANSWERED "NO" TO ANY OF THESE QUESTIONS, THEN THE CONTROLS DESCRIBED HERE ARE NOT JUST "NICE TO HAVE" BUT A "MUST HAVE" REQUIREMENT.



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. Appendix A contains additional information about key provisions of the Sarbanes-Oxley Act.

This paper addresses an area of particular concern to Risk Managers and one for which the Risk Manager has primary responsibility.

RISK MANAGEMENT AUDIT OF TPA SERVICES

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

Risk Managers employ TPA's to handle claims for reasons of professionalism, cost effectiveness, and flexibility. In particular, alternative risk financing options — including self-insurance, large deductibles, captives, retrospective and association programs — often use TPA's.

Because a TPA makes claim payments on behalf of its clients, Risk Management Departments must assess the design and

monitor the operation of the financial controls in place -- both internally and at the TPA – that assure accurate claim payments, medical bill repricing, fees, discounts and other charge and credit transactions. 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.

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 Type II SAS702/ 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 and systems at the TPA site(s). At a minimum, discrepancies identified in the SAS70 should be retested; if the TPA's SAS70 is out of date, qualified by the auditor, or nonexistent, then direct testing of TPA controls must be much broader in scope. 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 medical bill coding to specific clients and claims ... to be sure errors are found and corrected systematically.
4. Assess the design of the Risk Management Department's 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 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 & 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 procedures, including:

- Determining an adequate sample size that will produce reliable test results.
- Creating test data sets for analysis.
- Developing test plans and procedures that assure an accurate and comprehensive audit.
- Identifying and classifying exceptions.

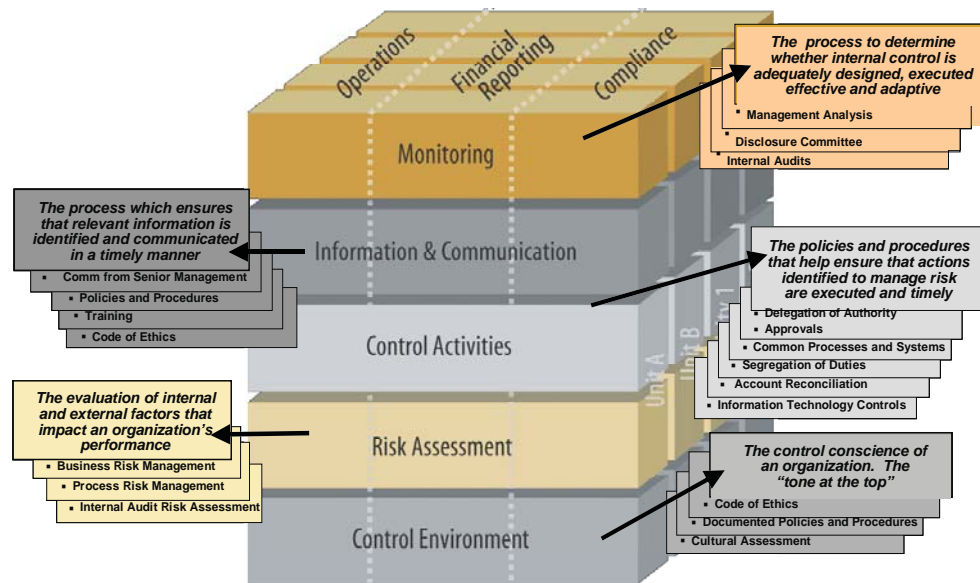
Controls found to be inadequate must be categorized as “deficient”, “significantly deficient”, or exhibiting a “material weakness”, depending upon the seriousness of the deficiency and the sums at risk. Deficient controls must be redesigned, installed and retested often until they prove effective.

FRAMEWORK FOR INTERNAL CONTROLS

While the Sarbanes-Oxley act does not specify a format for internal controls, many large public companies have adopted the control framework developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), which includes the following key elements:

1. Control Environment ... the overall system of governance, ethics, compliance and management processes that prevent fraud and assure accurate financial reporting
2. Risk Assessment ... formal process to identify significant accounts, processes, procedures and key controls in place
3. Control activities ... lists of individual control processes, procedures and tests performed at every company location, function and level of operation to assure accurate financial recordkeeping
4. Information and Communications ... information and documentation about control processes and results are communicated to and from management to promote efficient and effective operations.
5. Monitoring ... processes and procedures for periodic testing of key controls to assure they remain active and effective.

COSO Controls Framework



RISK MANAGEMENT DEPARTMENT CONTROLS OVER TPA SERVICES

A Risk Management department must establish its own system of processes and procedures so that controls do not simply become a “ritual”, but are kept up-to-date and fully operational.

1. Control Environment, Risk Assessment and Information & Communication: at the completion of an initial audit, basic information about these elements will be available. From this information, flow charts to illustrate critical risk elements and key control points can be developed.

- ⇒ Identify and assess critical risks, their probability of occurrence and potential losses.
- ⇒ Establish objectives for each process that clearly state what is to be achieved and how it reduces a critical risk.
- ⇒ Identify process owners, authorizers and other key personnel.

⇒ Identify how data is captured, processed and reported, and the significant dependencies on the integrity and availability of data.

2. Control Activities: an important element of control is a documented Standard Operating Procedure (SOP) for each process. An SOP for financial transactions must include the following elements at a minimum:

- ⇒ Authorization – including who may authorize, at what dollar levels, and for what types of transactions. Non-routine transactions and correction of errors should have separate authorization requirements.
- ⇒ Completeness and accuracy – routine and non-routine transactions must be classified and recorded properly.
- ⇒ Substantiation of balances— procedures that reconcile transactions to balances frequently enough to uncover and correct errors.

⇒ Data Integrity – systems and processes that “build integrity into” transaction data.

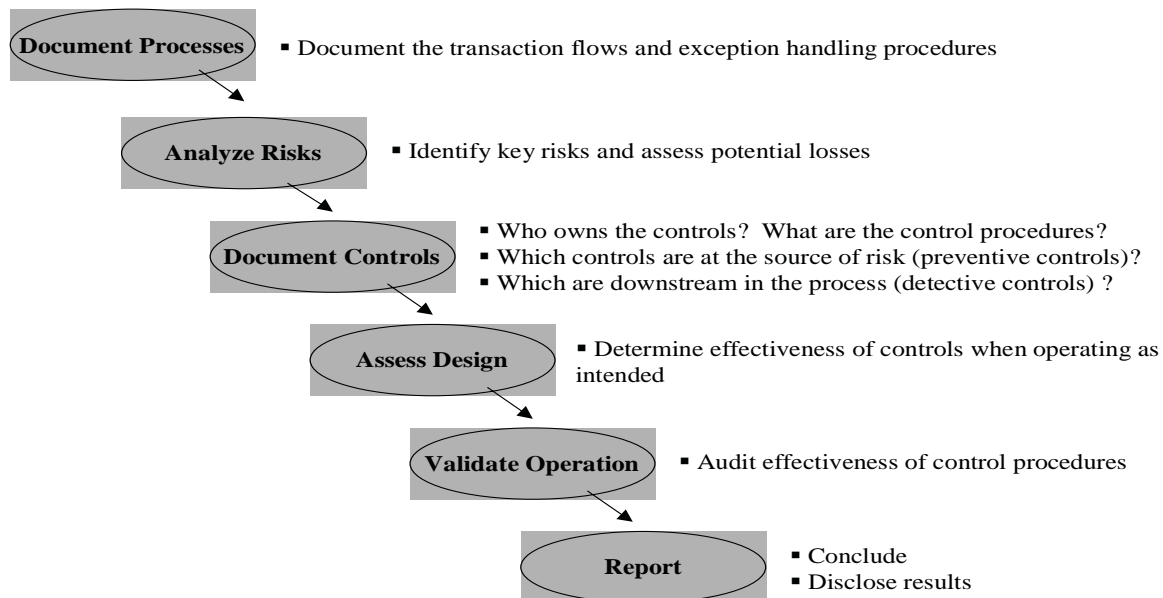
3. Monitoring Activities: processes and procedures are required for capturing, reporting and following up on deficiencies:

- ⇒ Monitor change, both internally & externally. Acquisitions, changes in personnel and system revisions at the TPA are some of the changes that require thorough retesting of controls.
- ⇒ Design and install a process to identify changes that may impact the adequacy of controls.
- ⇒ Develop analytics to handle data correctly and detect errors.
- ⇒ Create an array of reports detailing exceptions, audit results, limit violations and status of improvements, among others.
- ⇒ Set up timetables to validate controls and evaluate progress in correcting deficiencies on an ongoing basis.

This systematic approach to Sarbanes-Oxley opens up an opportunity. The integration of this work with two other quality control efforts—ScoreCarding and Claim File Audits—will enable organizations to save money and have a more effective view of their claim program. Claim file audits have a natural connection with the control processes described in this paper. Sarbanes-Oxley focuses on data and transaction integrity, while file audits address the core issue of whether the TPA is doing everything necessary to achieve the best resolution of claims.

ScoreCarding is a standards-based evaluation of how a company’s major operations and risk services vendors are performing over time. The creativity and effort required to define goals and to assess their payoffs is core to ScoreCarding. The performance of a company’s major divisions often involves objectives that, if met, may yield savings in the millions of dollars. Because you control the data, it avoids many of the challenges of benchmarking.

Steps for Managing TPA Controls



ONGOING MONITORING OF TPA AND USER FINANCIAL CONTROLS

To assure continuing credibility of financial controls, Risk Management Departments must adopt plans and procedures to periodically test all controls identified through an initial audit. Some examples of continuous monitoring include:

Input/Output comparison – compare all transaction information provided by the company to the TPA (such as social security numbers of claimants) to the information in the TPA's system on a regular basis, so keying errors may be found and corrected. Are these your employees and your claims?

Performance indicators – check all specific performance measures specified in contracts, special instructions and written “best practices” 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 – set up user controls to review and reconcile TPA invoices and analyze discounts, fees and special charges and credits 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 – perform periodic analysis of large payees, identification of “repeat” claimants, and other measures necessary to uncover improper payments.

Exception Procedures – establish a review process for manual transactions that involve correction of errors or “special events” using someone not a party to the original transactions.

CONCLUSION

The Sarbanes-Oxley Act affects large public companies and all of their important operations. Because of the specialized risks and systems involved with TPA's, 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. Sarbanes-Oxley compliance is mandatory, but an organization can gain efficiency and savings by combining the Sarbanes-Oxley review with Claim File audits and ScoreCards for its major divisions and vendors.

APPENDIX A

KEY PROVISIONS OF THE SARBANES- OXLEY ACT

SECTION 302

CORPORATE RESPONSIBILITY FOR FINANCIAL REPORTS

CEO's and CFO's must personally certify that they are responsible for disclosure controls and procedures and that the report they are issuing is accurate, complete and fairly presented.

Quarterly and annual filings with the SEC must contain a certification that the CEO and CFO have performed an evaluation of the design and effectiveness of the disclosure controls.

Certifying executives must state that they have disclosed to their audit committee and independent auditor any significant control deficiencies, material weaknesses or acts of fraud, and significant changes in financial reporting internal controls.

SECTION 404

MANAGEMENT ASSESSMENT OF INTERNAL CONTROLS

The company must perform an annual evaluation of internal controls over financial reporting, and a quarterly evaluation of any material change in the company's internal controls that occurred during the fiscal quarter.

The company's independent auditor must issue an attestation report on management's assessment of the effectiveness of internal controls over financial reporting

Annual filings must contain a report by management on their assessment of the effectiveness of internal controls over financial reporting. 4/

The concern addressed by Sarbanes-Oxley in general, and Section 404 in particular, is that issuers of publicly held securities

provide assurances to the holders of those securities that:

- The issuer has processes in place that provide reasonable assurance that transactions are properly authorized;
- The issuer's transactions are properly recorded and reported; and,
- The issuer's assets are safeguarded against unauthorized or improper use.

Effectively designed and operating controls and procedures require an infrastructure of policies, processes, people, reports and systems – for the business as a whole, and for each important business unit and operation.

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 over a period of time, that if incorrect would potentially cause the company's financial statements to be false or misleading. As a rule of thumb, \$1,000,000 would generally be considered "significant" for a Fortune 1000 company.

2/. A Type II SAS70 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 all processes and controls that are relevant to the service organization's clients.

3/. "What Color Are Your Sox?" M. Kinney, Presentation, October 15, 2004.

4/. "Sarbanes-Oxley: The IT Dimension", S. Chan, Internal Auditor Magazine, February, 2004.

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



Gallagher Bassett Services, Inc.

www.gallagherbassett.com

About Gallagher Bassett Services, Inc.

Gallagher Bassett is the largest multi-line property/casualty third-party administrator, offering enlightening insights and services in the areas of claims management, information management, medical cost containment, risk control consulting, and appraisal services.

The Gallagher Centre
Two Pierce Place
Itasca, IL 60143
1-630-773-3800



www.shelterislandrisk.com

About Shelter Island Risk Services

Shelter Island Risk Services (SIR) is a technology firm serving the Risk Managers from public, private, and government organizations.

We also improve the ability of Claim Administrators, Insurers, Brokers, and other Risk Services providers to deliver technology to their clients.

P.O.Box 568
Shelter Island, NY 11964
1-800-749-1535