

eReinsure

Sarbanes-Oxley Compliance

8/24/2004

The Sarbanes-Oxley Act

The Sarbanes-Oxley Act of 2002, overseen by the U. S. Securities and Exchange Commission (SEC), implements safeguards against accounting errors and fraudulent management practices. This legislation was drafted and passed in direct response to the Enron scandal and other corporate accounting scandals in 2001 and 2002. It is arguably the most significant single piece of legislation impacting public corporations since the U.S. securities laws of the 1930's. In passing the Sarbanes-Oxley Act, Congress recognized that strong internal controls are a critical component of accurate financial reporting. Section 404 of Sarbanes-Oxley explicitly requires the CEO and CFO to be accountable for their company's system of internal controls. In addition, the external auditor must perform testing to validate management's assessment of these internal controls. If a material weakness is found, new guidance requires that the auditor issue an adverse opinion.

Why is reinsurance process likely to come under scrutiny?

Recent events have focused far greater attention on reinsurance and the potential impact of reinsurance on insurers' results. As of year-end 2002, the last year for which S&P has full-year data, reinsurance recoverable assets represented approximately 60% of the aggregate surplus of the p-c industry, up from about 30% just five years earlier¹. One recent study found that as recoverables have grown, so has the gap between cedent and reinsurer expectations. The rate of recoverables growth slowed from its 29% high in 2001 to 6% in 2003, yet the aggregate recoverable gap continued to grow at a 22% rate in 2003².

Legacy issues demonstrate the dangers of inadequate documentation and control of reinsurance. When combined with the vagaries of the tort system, insurance market cycles and equity market fluctuations, uncertainty around reinsurance creates significant financial stress in the insurance system. The adoption of improved internal controls can ensure that complete information is captured for future transactions. The management of future recoverables requires the parties to

¹ *Standard & Poor's*

² *Conning Research*

“trap a transaction” at inception – with a full audit trail to evidence the disclosures and the agreement.

Even when a transaction complies with appropriate standards for contract formation and documentation, counter party credit risk is an issue that will require active management and readily accessible information on aggregations. Information on where reinsurance is placed must be timely and complete. Insurers must be able to control where reinsurance is purchased and manage this process dynamically in a constantly changing marketplace.

Internal controls

Sarbanes-Oxley compliance is not just an event, but rather a process. The SEC is expected to continue interpreting the Act and issuing new rules defining what will be required. Many companies can simply find themselves overwhelmed by the scale, complexity and, not least, cost of implementation in areas ranging from documentation to data collection³.

In most companies of any size, data moves between multiple business groups and IT systems on its way from initial transactions to the reports that the CEO and CFO must attest to. While the SEC has required that a system of internal controls must conform to a recognized and accepted framework it hasn't mandated use of any particular standard. Infact, it is important for management to understand that multiple principles and frameworks will be relevant (see appendix). Sarbanes-Oxley Section 404 attestation requires auditors to understand transactional processes as well as management confidence in the systems that house, move, and transform data. This confidence is critical in the area of IT controls given their pervasive effect on the achievement of many other control objectives.

The framework for controls

One example of a process framework is the IT Governance Institute's Control Objectives for Information and Related Technology (COBIT). This is used by many IT professionals to evaluate their systems of internal controls and represents a proven roadmap for compliance. Among the multiple phases are two categories of information system control activities, general controls and application controls.

- a. General controls apply to all information systems and support the secure and continuous operation of the entire entity. In evaluating these controls, ask yourself questions such as:
 - i. “Do you have policies and procedures in place?”
 - ii. “How do you manage changes?”
 - iii. “How do you ensure system and data security?”
 - iv. “How do you manage problems and incidents?”

³ *PriceWaterhouseCoopers – ERM for the Insurance Industry – Global Study*

- b. Application controls include those designed to prevent unauthorized transactions and record and monitor transactions. In evaluating these controls, ask yourself:
 - i. “Do you know that transactions are properly approved and within authorization limits?”
 - ii. “How do you know that unauthorized transactions are rejected?”
 - iii. “Are all transactions captured by the system and recorded in the proper period?”
 - iv. “How do you know that there is a method to identify missing transactions?”

eReinsure as a process control for reinsurance

The management of reinsurance includes many components that must be considered in Sarbanes-Oxley Section 404 attestation. Risk assessment under the COBIT framework requires consideration of whether the potential for a control failure is more than remote, and second, the impact to the organization if a control break actually occurs. Organizations with multiple locations also must assess risk associated with these various processing locations.

Failures common to the reinsurance transaction include:

- i. Inadequate disclosure
- ii. Unapproved counter parties
- iii. Incomplete documentation and audit trail
- iv. Misplaced records
- v. Inability to associate the reinsurance contract with a primary policy at the time of a claim
- vi. Inability to access information to control aggregation of counter party risk
- vii. Inability to reconcile premium accounts and make / receive timely payments
- viii. Errors due to the re keying of data

The eReinsure negotiation platform represents a structured workflow for the placing of individual risk and automatic reinsurance. The system is a highly reliable, secure, and proven data repository and workflow platform that is accessed over the internet. The system architecture provides for customer data to be secured in a “state-of-the-art” data centre and yet be accessed from any PC via a browser interface.

By standardizing workflow and centralizing information, eReinsure gives reinsurance buyers, sellers, and brokers the ability to arrange risk financing solutions, reduce redundant effort and ensure greater speed and accuracy in reinsurance negotiation. Throughout the process, each party has online access to real-time information on the progress of the negotiations. The eReinsure platform also supports integration with legacy systems, reducing the re-keying of data and providing control of the source and destination of data.

The way forward

Sarbanes-Oxley Section 404 has been described by some as a “sudden and blunt instrument” to achieve the objective of improved corporate governance. However, as William Donaldson, SEC Chairman has commented: *“If companies view the new laws as opportunities – opportunities to improve internal controls, improve the performance of the board, and improve their public reporting – they will ultimately be better run, more transparent, and therefore more attractive to investors”*. The bottom line is that the business environment has changed and process control demands improved systems to support increased accountability. Superficial compliance with Sarbanes-Oxley is not an option and management at all levels must become ever more familiar with internal control practices.

This is not a complete description of the many requirements under the Act, but is provided to illustrate the scope and nature of the regulation. Each organization should carefully consider the appropriate IT control objectives for its own circumstances. Therefore, organizations should consult with their own legal and compliance experts to determine what they must do to comply. Non-compliance presents a significant risk, with fines ranging into the millions, as well as potential criminal penalties.

Appendix

Frameworks and Principles for Sarbanes-Oxley Section 404 Compliance

In addition to the IT Governance Institute's Control Objectives for Information and Related Technology (COBIT) referenced above, additional illustrative control activities are provided by the following:

The Committee of Sponsoring Organizations of the Treadway Commission

Recognizing the need for definitive guidance on enterprise risk management, The Committee of Sponsoring Organizations of the Treadway Commission (COSO) initiated a project to develop a conceptually sound framework providing integrated principles, common terminology and practical implementation guidance supporting entities' programs to develop or benchmark their enterprise risk management processes. The resulting framework serves as a common basis for managements, directors, regulators and others to better understand enterprise risk management, its benefits and limitations, and to effectively communicate about enterprise risk management issues.

US Public Company Accounting Oversight Board

The PCAOB (US Public Company Accounting Oversight Board) standard includes specific requirements for auditors to understand the flow of transactions, including how transactions are initiated, authorized, recorded, processed and reported. Such transaction flows commonly involve the use of application systems for automating processes and supporting high volume and complex transaction processing. While general in nature, these PCAOB principles provide direction on where SEC registrants likely should focus their efforts to determine whether specific IT controls over transactions are properly designed and operating effectively.

Contact eReinsure

Salt Lake City

424 East 500 South
Suite 104
Salt Lake City, Utah 84111
USA

Main: +1.801.521.0600
Fax: +1.801.521.0601
sales@eReinsure.com

New York

1251 Avenue of the Americas
19th Floor
New York, NY 10020
USA

Main: +1.212.474.9482
Fax: +1.212.474.9401

London

Suite 820, Lloyds Building
1 Lime Street
London, EC3M 7HA
England

Main: +44(0)20.7327.3555
Fax: +44(0)20.7327.3556

www.eReinsure.com