

Optimum Performance with Audit Standard 5

By Patrick Taylor

To mitigate the load felt by almost every company complying with SOX, the SEC released new guidance known as Audit Standard 5, which takes a more risk-based approach to auditing.

Companies have been building compliance efforts since Congress passed the Sarbanes-Oxley Act (SOX) in 2002. However, the transition for many companies has not been smooth. Organizations began by factoring check lists into numerous processes and soon became burdened with the seemingly endless SOX requirements. Even worse, companies failed to avert the fraud these requirements were supposed to address.

SEC Chairman Christopher Cox said, “Congress never intended that the 404 process should become inflexible, burdensome and wasteful. The objective of Section 404 is to provide meaningful disclosure to investors about the effectiveness of a company’s internal controls systems without creating unnecessary compliance burdens or wasting shareholder resources.”¹

Nevertheless, to mitigate the load felt by almost every company complying with SOX, the SEC released new guidance known as Audit Standard 5 (AS 5) which takes a more risk-based approach to auditing.

“With the Commission’s new interpretive guidance for management on the evaluation and assessment of its internal controls over financial reporting, companies of all sizes will be able to scale and tailor their evaluation procedures according to the facts and circumstances,” Cox said. “And investors will benefit from reduced compliance costs.”²

What does AS 5 mean?

AS 5 makes compliance more efficient by taking a risk-based approach, allowing companies to evaluate where to place their control emphasis. Instead of covering all fraud scenarios, companies can dedicate their resources to preventing fraud where it is most likely to occur. Organizations still achieve the goal of preventing fraud without wasting time and money

chasing down remote possibilities of fraud, regardless of likelihood or potential impact.

For example, rather than committing resources to document the security around backup tape procedures, a company can devote resources to monitor journal activities to identify any management override of controls. By identifying and focusing on areas of highest risk, companies can prevent fraud that might otherwise have slipped through unnoticed. The largest losses to investors have come from management “cooking the books,” not from someone restoring data from manipulated backup tapes.

AS 5 stresses reliance on the work of internal audits, eliminating the need to recheck already accurate assessments. Auditors can look at collected reporting data, and while it shows them everything they need to know, they still need to go through the process of creating the same report for their own use. With the new guidance, external auditors can depend on well-documented results to direct time and energy, reducing costs and duplication of work. One way for companies to establish well-documented information is to use a continuous monitoring system which summarizes problems and what solutions have been implemented to mitigate the issues.

Risks to address with AS 5

SOX was created to prevent repeats of scandals such as those at Enron³ and Tyco.⁴ However, companies like Dell proved that SOX was not enough to stop these scandals. Organizations are struggling to address threats in a low-cost and effective manner, and AS 5 hopes to help. The struggle has been, in large part, due to a lack of clarity regarding the true risk. Auditors should focus efforts in the highest-risk areas as determined by a risk analysis.

Some of the risks AS 5 hopes to address include the general ledger (GL). With most companies, the highest risk for fraud

1 “SEC Approves New Guidance for Compliance with Section 404 of Sarbanes-Oxley,” Securities and Exchange Commission. May 23, 2007. <http://www.sec.gov/news/press/2007/2007-101.htm>.

2 *ibid.*

3 “Behind the Enron Scandal,” TIME, <http://www.time.com/time/2002/enron>.

4 Securities Fraud FAQs: <http://www.lawyershop.com/practice-areas/criminal-law/white-collar-crimes/securities-fraud/faqs>.

involves the GL. Within the GL there are always adjustments that need to be approved. Privileged users can revise account balances without causing comment. However, this is where abuse can arise through otherwise valid adjustments.

For example, management can either use its own override capabilities to bypass journal entry controls or pressure subordinates to make entries contrary to policy. Additionally, management can attempt to override revenue recognition policies through either direct entry or by pressuring subordinates. Another way to misuse power is for authorized users to go around corporate policy and journal entry controls by splitting single manual entries into multiple manual entries, each of which individually falls within policy restrictions.

Benefiting from AS 5

Companies can maximize the benefits from the shift to AS 5 by re-evaluating current compliance efforts to remove some dead weight. This will allow companies to prioritize risks and respond accordingly with more resources to devote to the most likely causes of fraud.

In addition, companies should consider employing a continuous transaction monitoring solution. To combat the highest risk areas, companies should not settle on a random sample of transactions. Automated continuous monitoring allows companies to routinely check all single financial transactions for fraud. Reducing the user error that comes with inaccurate data entry improves the chances of catching fraudulent activities, while saving overhead and eliminating duplicate payments and other errors in the billing process.

Deliberating a risk-based approach

It can be nearly impossible to comprehensively prevent all potential fraud scenarios. Effective prevention involves finding the greatest risks. In a 2008 report on Sarbanes-Oxley, Oversight Systems found identifying the areas of greatest risks is the number one concern of financial executives surveyed.⁵ Financial transactions in a company require privileged users to manage unique situations that inevitably arise. With these user override capabilities, companies have had to diminish their “firewalls.” This requires a shift in tactics for preventing fraudulent practices.

With a process already in place for addressing problems, companies need to monitor all GL transactions for fraud risk. Today, company policy might require all manual journal entries greater than a specific dollar amount to be reviewed and approved by the controller. However, with AS 5, auditors will evaluate all entries in areas of greatest risk, including automated entries – companies need to ask themselves, “Is our current policy adequate to address fraud risk?”

With AS 5, auditors can base their judgments on the systems already in place. Developing this sort of risk-based approach will help companies highlight the measures they have taken

to decrease risk when they are audited. This minimizes the potential for misstatements and fraud from management overrides.

With the higher potential for management fraud, a company can focus more effort in this area. With developed checklists and controls, changing to AS 5 should be a smooth transition because companies have already spent years developing checklists of controls. Previous guidance was more cover-all-the-bases approach, focused on making sure a company had a plan in place. Under AS 5, companies do not have to expend much time attending to unimportant details and instead can emphasize their fraud risk assessment.

Cutting fraud and compliance costs

To combat fraud and lower compliance costs, companies must consider the fraud diamond, which includes the following elements: reasoning, strain, opportunity, and capacity.

Reasoning

Anyone involved in fraudulent behavior can commit illegal actions he does not perceive as being in conflict with personal ethical standards. In many cases, individuals started out “stretching” company policy. Over time, their activities continued to shift further from appropriate behavior. Effective fraud prevention must assist the individual’s ability to recognize appropriate values and actions. When even “shades of gray” are highlighted as noncompliant, it makes it harder for individuals to begin the slide into outright fraud. Continuous monitoring can flag potentially fraudulent actions that are exceptions to accepted policy and controls and raise individuals’ consciousness of potential ethical conflicts.

Strain

Reducing fraud risk can be applied to general company policies. One of the precursors to fraud involves tying compensation closely to financial performance. Oversight found 81 percent of corporate fraud occurs because of the pressure to do whatever it takes to meet goals.⁶ If this business structure is necessary, companies need to have independent controls over management overrides to reduce this risk.

Opportunity

Companies need to evaluate whether controls are sufficient to address the risks of fraud, especially regarding management override. One of the most effective ways to do this is to implement a continuous monitoring solution. Continuous monitoring is a control that observes the effectiveness of other controls by testing every transaction. If a company’s continuous monitoring program includes the processes for dealing with errors and other problems, then the company is able to detect and prevent misstatements on a timely basis. Under AS 5, if other control activities do not prevent misstatements of financial information, or if they only remove a remote op-

5 “The 2008 Oversight Systems Financial Executives Report on Sarbanes-Oxley,” July 29, 2008. http://www.oversightsystems.com/resources_reports.php.

6 “The 2007 Oversight Systems Report on Corporate Fraud,” June 11, 2007. http://www.oversightsystems.com/resources_reports.php.

portunity for fraud, companies may consider removing the activities as key controls.

Capacity

As employees learn the intricacies of a company's financial system, those who can potentially commit fraud gain confidence in their ability to do so. Under AS 5, companies can focus their attention on the areas where fraud is most likely to occur. As employees learn what steps to take in order to remain hidden, companies need to understand that auditing only a sample of transactions leaves them vulnerable to fraud because fraud consists of singular events that can be impossible to find through a sample.

Preventing fraud in the future

Under AS 5, organizations can focus compliance efforts where they will do the most to prevent errors and fraud. Using continuous monitoring and honing controls to address risk can reduce employees' capabilities and opportunities to commit fraud. Adjusting company policies to eliminate un-

reasonable performance pressures may reduce risks associated with management override of controls. Continuous monitoring not only aids in the detection and prevention of financial misstatements, it minimizes personal rationalizations that lead otherwise trustworthy employees to perform fraudulent actions.

By implementing effective solutions and industry best practices, companies can help ensure they and their employees meet compliance requirements.

About the Author

Patrick Taylor, CEO of Oversight Systems, previously held leadership roles at ISS, Symantec, Oracle, Red Brick Systems, GO, Air2Web and Fast-Talk. He has a Bachelor of Mechanical Engineering with honors from the Georgia Institute of Technology and an MBA from the Harvard Graduate School of Business Administration.

