Focus on High-risk Controls

The PCAOB's Auditing Standard No. 5 enables publicly listed companies to narrow the scope of testing for Sarbanes-Oxley compliance.

BY DANNY M. GOLDBERG

WITH THE ADOPTION OF THE U.S. PUBLIC Company Accounting Oversight Board's (PCAOB's) Auditing Standard No. 5 (AS5), publicly listed companies could reduce compliance testing for the U.S. Sarbanes-Oxley Act of 2002 to a more manageable level. Internal audit departments should benefit as testing can be scaled back with increased reliance on entity-level controls and the re-assessment of key controls in the internal control environment. This presents an opportunity for organizations to review their current internal control structure and focus on high-risk processes and controls.

AS5 places greater emphasis and reliance on entity-level controls than its predecessor, Auditing Standard No. 2 (AS2), in two ways. First, entity-level controls assist internal and external auditors in tailoring the audit through a top-down approach in AS5. Additionally, the new standard makes effective entity-level controls tantamount to an effective internal control structure. Depending on the circumstances, AS5's focus on entity-level controls allows auditors to reduce the scope of testing controls at the process level, which can profoundly reduce the amount of testing by companies and external auditors alike.

The most important aspect of AS5 is the PCAOB's emphasis on risk assessment in the audit of internal control. The board, however, did not specify whether risk should be assessed at the financial statement/assertion level or by individual control. The PCAOB continues to assert that the auditor may vary the nature, timing, and extent of testing based on the risk.

RISK ASSESSMENT PROCESS

A company has choices in the form of risk re-assessment it can undertake to comply with AS5. The assessment can be assertion-based, which is more of an overall assessment of significant processes and transactions inherent in the company's control structure. Companies with limited Sarbanes-Oxley compliance experience or companies that want to start over in assessing their current control structure would choose this method. However, the assertion method could be counter-productive for firms that understand which major transactions and balances pose the greatest risk.

Alternatively, companies can complete a more detailed re-assessment of each control currently identified as key. This method is less costly and takes less time than the assertion-based assessment. Moreover, it relies on the current control structure the company has identified, rather than scrapping previous work.

An IIA Global Audit Information Network (GAIN) survey issued in September found that 74 percent of respondents are combining these two types of risk assessments. This hybrid tactic provides the advantages of each method, while possibly eliminating certain audit areas based on risk and materiality. Companies using this hybrid methodology assess risk via a top-down linkage to financial statements, identify the high-risk areas and relevant entity-level controls, and assess risk on a control level (controls prioritization). Assessing risk at the control level requires a three-step approach.

1. RE-ASSESSMENT OF KEY VERSUS NON-KEY CONTROLS Companies that assist their external auditors with compliance testing should use AS5 to refocus the current control structure on key impact controls. The first step in this process ideally should take place during the first part of the fiscal year. The company can review its current control structure and, based on three to four

years of previous experience, re-identify key controls. Eliminating previously identified controls may involve removing duplicate controls, controls that should be secondary controls but were previously misidentified, and controls that are ineffective or pertain to risks that have been mitigated through other controls. The most effective ways to undertake this process are to conduct walk-throughs with members of each area present to assist in the process and to perform control self-assessment workshops sponsored by management.

2. ASSESSMENT OF INDIVIDUAL KEY CONTROL RISKS The next step in the process is formalizing a rating procedure and placing a risk rating on each control. Because classifying risks into three categories — high, medium, and low — is very subjective, the company should strictly identify the criteria for each classification. A sound methodology can be formulated easily based on the general guidance contained in AS5:

- *High* — A control that is linked to more than five risk assertions ("what could go wrong" questions). Additionally, controls that are overall monitoring controls and are valued in numerous processes are classified as high, as are controls that had significant findings in previous years.
- *Medium* — Controls that had minimal or no findings in previous years, but are necessary to test and integral to the process.
- *Low* — Controls that did not have findings in the previous year's testing and have not had changes in how they operate or in the personnel performing the controls. Also, controls that are inherent in the current control environment, but are unlikely to cause a material misstatement.

Essential to this assessment of individual key control risks is the competence and reliability of company personnel who perform the controls and test them. Otherwise, the risk assessment could be deemed useless, and relevant areas would all be high-risk.

3. RE-ASSESSMENT OF THE TESTING SCOPE BASED ON AS5 The final step in the re-assessment process is determining the

Control Prioritization Model

	HIGH RISK	MEDIUM RISK	LOW RISK
Initial Testing	No change in testing from previous year.	No change in testing from previous year.	Narrow sample size by one frequency category.
Update Testing	No change in testing from previous year.	Walk-through.	Walk-through.

amount that testing can be decreased. Companies can re-assess the testing scope using a control prioritization model that specifies the scope of initial testing and update testing for high-, medium-, and low-risk controls (see "Control Prioritization Model" on page 70). The new testing scope should decrease initial and update testing of low-risk controls. Update testing should also decrease for medium risks if no findings or significant issues are identified. However, companies should maintain the same testing scope for high-risk controls they had in previous years.

CONTROL PRIORITIES

"Control Prioritization Examples," on this page, illustrates how different types of controls are treated under the control prioritization model. These can be reviewed based on their risk classification — high, medium, and low.

HIGH The first control (expense report review) is listed as high risk due to many factors, including issues identified in prior-year test results and changes in the process and personnel. Any of these factors alone might not result in a high rating, but together they would be a high risk in most cases. Review of balance sheet reconciliations is a high risk because it is a significant monitoring control for a company, according to AS5.

MEDIUM These controls are deemed significant and key to each related significant process but would be difficult to classify as low or high risk. For example, appropriate approval of time reports would not be classified as high risk, regardless of prior-year findings, unless the majority of employees were hourly and the findings and materiality were significant. Conversely, appropriate approval of employee action forms is a key control that most likely would not be classified as low risk due to the significance of the control in most companies.

LOW Both of the controls that are labeled low risk are inherent in the process in most cases. The controls are easy to test, and a finding in this area would usually be easy to correct.

Although companies can vary their control risk assessment, it is important to apply a conservative approach consistently. Additionally, control risk classification will differ from company to company due to the inherent control environment and other factors.

A RETURN TO BALANCE

Many companies are already seeing benefits from the risk-based focus on key controls specified in AS5. In the September GAIN survey, 59 percent of early AS5 adopters reported that their organization has decreased the scope for initial testing by between 11 percent and 50 percent. By using AS5 to their advantage, companies and internal auditors have an opportunity to narrow the focus of Sarbanes-Oxley compliance testing and redefine internal audit objectives for better balance.

DANNY M. GOLDBERG, CPA, CCSA, is director of internal audit for Tyler Technologies in Dallas.

To comment on this article, e-mail the author at danny.goldberg@theiia.org.

To share emerging risk issues and best practices from your own audit experiences, or to request coverage of a particular risk, e-mail jamesroth@audittrends.com.

Control Prioritization Examples

Control Description	Findings in Previous Year?	If Yes, Were Any Significant?	Has the Process Changed?	Have the Personnel Changed?	Risk Rating
Before payment, the division accounting department reviews expense reports for ledger account coding.	Yes	No	Yes	Yes	HIGH
Balance sheet reconciliations are reviewed monthly by the controller.	No	N/A	No	No	HIGH
Access to personnel files at each division is limited to appropriate individuals.	No	N/A	No	Yes	LOW
A formal approval by the immediate supervisor or department head is required for all time recorded by all hourly employees.	Yes	No	No	No	MEDIUM
For all employee status or rate changes, an employee action form is approved by the applicable supervisor.	No	N/A	No	No	MEDIUM
Prenumbered purchase orders are used for all items of cost and expense.	No	N/A	No	No	LOW