The ABCs of Reporting on Controls

Could a top-down, risk-based approach be applied to management's assessment of internal control over financial reporting?

BY BRUCE MCCUAIG

EVERY HUNGRY VISITOR TO LOS ANGELES County, on entering a food service establishment, is greeted at the door with a poster showing the letter A, B, or C in large colored print. The letters represent an estimation of the residual risk to one's health of dining in that establishment as determined by a Los Angeles County health inspector. The poster tells potential diners if the individual establishments have superior, good, or only acceptable food handling practices as well as the level of their overall facilities maintenance.

Los Angeles County has developed a tool that the U.S. Securities and Exchange Commission (SEC) and Public Company Accounting Oversight Board (PCAOB) have long advocated but still struggle with implementing — a top-down, risk-based approach to control effectiveness and an innovative reporting philosophy. The health inspectors know, in detail, the inherent risks of every type of foodborne illness. The framework for evaluating control effectiveness is based entirely on a top-down assessment of risks. For example, using statistics published by the Centers for Disease Control (CDC), health inspectors know that 63 percent of foodborne illness outbreaks are a result of risks associated with "inadequate cooling and cold holding temperatures." They also know the frequency of every other type of risk of foodborne illness — from staff hygiene to contaminated raw ingredients.

The health inspectors provide the management of food service establishments with guidance on control standards to mitigate these risks. They have developed a clear set of criteria to guide food establishment owners on what food handling and facilities maintenance standards are required to manage specific risks, and they explain exactly how their conformance to those standards will be measured. A Food Official Inspection Report (FOIR) has been designed to identify and point-score restaurants on their compliance with health standards. The FOIR's intent is to "recognize the varying degrees of risk associated with violations of the applicable laws, codes, and regulations." Points are deducted for noncompliance, and a specific letter grade is assigned accordingly.

Finally, the Los Angeles County Health Department uses a simple but highly innovative reporting philosophy based on residual risk. The health inspectors do not issue an opinion on the "effectiveness" of controls over food safety. Instead, they assess the residual risk associated with a food service establishment based on a set of criteria and a scoring system for evaluating the mitigation of inherent risk. They are letting diners decide for themselves if the residual risk is acceptable. It is clear that more residual risk is associated with a C restaurant than an A restaurant; however, the price may compensate for the difference in risk.

Compared to regulating food safety in restaurants, assessing and reporting on internal control over financial reporting in public companies is much more complex. However, the basic principles should be the same. Specifically, accountants, auditors, senior executives, and the regulatory community should start by asking, "Where are the known risks, what steps have proven effective in mitigating the known risks, how should conformance to those mitigating activities be measured, and what should be reported to the public?"

In the world of internal control over financial reporting, regulators and auditors are struggling to understand and adopt a risk-based approach. In its May 16, 2005, Staff Statement on Management's Report on Internal Control Over Financial Reporting, the SEC concluded, "in many cases neither a top-down nor a risk-based approach was effectively used" by the public accounting profession. This theme has been repeated in subsequent SEC statements on the implementation of Section 404 of the U.S. Sarbanes-Oxley Act of 2002. Rather than focusing first on understanding known risks to financial reporting, external auditors, according to the PCAOB, have been focusing on documenting and verifying controls. The connection between controls verified and risks mitigated is implicit at best. Conversely, the CDC produces risk statistics based on studies of foodborne illness. Los Angeles County health inspectors know precisely what temperatures are required to keep food from contamination and what facilities are required to maintain those temperatures.

Unlike a reporting framework based on assessing and scoring residual risk, Sarbanes-Oxley requires a simple pass or fail reporting framework. An analogy to the Los Angeles system is that unless the health inspectors have closed the establishment, we must assume things are OK. Under Sarbanes-Oxley rules, a company has effective internal controls over financial reporting or it has a material weakness, in which case its internal control over financial reporting is ineffective. What we don't know is whether the company is right on the borderline of an ineffective internal control system or whether it is superb. Excellence in implementing an internal control framework is not rewarded.

Can a grading system be applied to management's assessment of internal control over financial reporting to let investors know just how good, or bad, a company's internal control framework is? No less an authority than the California Public Employees Retirement System (CalPERS) has called for one. In their response to the exposure draft of PCAOB Auditing Standard No. 2 they wrote, "We believe that the opinion on management's internal control assessment should have a graded scale rather than simply pass or fail."

What would the grading system look like? Essentially a residual risk-based

Los Angeles County Health Inspector Ratings

A Generally superior in food handling practices and overall food facility maintenance.

B Generally good in food handling practices and overall food facility maintenance.

C Generally acceptable in food handling practices and overall general food facility maintenance.

Sample Residual Risk Index

0 Fully Acceptable
No unacceptable issues. No additional attention or corrective actions required at the current time.

1 Low
Inaction on issues could result in minor financial reporting errors. Routine attention required to adjust status to an acceptable level.

2 Moderate
Inaction on issues could result in, or will allow continuation of, mid-level financial reporting errors. Moderate effort required to adjust status to an acceptable level.

3 Significant
Inaction on issues could result in, or will allow continuation of, serious negative impacts on financial reporting. Attention required immediately to adjust status to an acceptable level.

4 Major
Inaction on issues is virtually certain to result in, or allow continuation of, major negative financial reporting errors. Analysis and corrective action required immediately.

5 Severe
Inaction on issues is virtually certain to result in, or allow continuation of, severe negative financial reporting errors or conditions. Senior management-level attention and board reporting is urgently required.

6 Catastrophic
Inaction on issues will result in, or allow continuation of, catastrophic financial reporting errors. Senior management- and board-level attention is urgently required to avert a catastrophic negative impact.

7 Terminal
The current status of financial reporting errors is extremely material and negative and having disastrous impact on the organization's future. Immediate top priority action from the board is necessary.

system would provide more detail on the level of residual risks existing in a company's internal control over financial reporting. Residual risk — the level of risk remaining after considering the effectiveness of controls in place — could be associated with an entire reporting framework, with individual processes, financial statement line items, or organization entities.

A score of greater than three would be strong evidence of a significant deficiency when applied to an individual disclosure. A score of greater than five would be strong evidence of a material weakness when applied to an individual disclosure, and the overall system of internal control would likely be considered ineffective. A rating system could be applied to the entire organization. Credit rating agencies have developed standards that score entire companies using a letter scale. The scale is carefully defined, well understood, and tested for reliability. Although it's not foolproof — many credit rating agencies were fooled by the Enrons and WorldComs of the last decade — on the whole, the system has provided more objective guidance than a simple pass/fail system.

A grading system would provide more detail on the level of residual risks existing in a company's internal control over financial reporting.

According to a report published by Moody's Investors Service, The Second Year of Section 404 Reporting on Internal Control, "Reports citing material weaknesses have become lagging rather than leading indicators of financial reporting problems." The report suggests that management and auditors require evidence of a material error before they are willing to conclude that a material weakness exists. That is comparable to a health inspector waiting for evidence of food poisoning before taking action to protect the public. It is not acceptable in the food safety business and it should not be acceptable in reporting on internal control over financial reporting.

BRUCE MCCUAIG, CIA, CCSA, is a principal consultant with Paisley Consulting, a Cokato, Minn.-based business accountability solutions firm.

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