Internal Audit and SOX on a Budget

By Adam J. Epstein and Sonia Luna

Adam J. Epstein advises pre–IPO and small-cap boards through his firm, Third Creek Advisors LLC. He is the author of *The Perfect Corporate Board: A Handbook for Mastering the Unique Challenges of Small-Cap Companies* (McGraw-Hill, 2012). **Sonia Luna**, CPA, is the founder of Aviva Spectrum. She has more than 18 years of compliance and internal and external audit experience, and was recently appointed by SEC Chair Mary Jo White to the Advisory Committee on Small and Emerging Growth Companies.

It's been more than 10 years since the New York Stock Exchange began requiring all listed companies to maintain an internal audit function. In 2013, Nasdaq proposed a similar rule, but withdrew it several months later. A review of some of the public comments submitted to the Securities and Exchange Commission (SEC) regarding Nasdaq's proposal highlights concerns regarding the one-size-fits-all applicability to smaller listed companies. For example:

- The Society of Corporate Secretaries and Governance Professionals commented that it "is not aware of any analysis of the cost and burdens of the proposed rule on Nasdaq-listed companies generally, and on smaller companies in particular."
- The chief financial officer of Cytokinetics commented: "As a CFO of a small biotechnology company with 74 employees and a market cap of $150m and no material or consistent revenues, this requirement is another example of the agency applying a one-size-fits-all view. This requirement will be another financial burden added to the already mounting burden that is being placed on smaller companies today to remain compliant with regulatory requirements."
- The chief financial officer of Northern Technologies International Corp. noted: "We have an accounting and finance staff of four people (two clerks, a controller, and me). It is overkill to now have an internal audit requirement, on top of the already burdensome SOX [Sarbarnes-Oxley Act of 2002] compliance that we already put in place."

The focus on financial burden is common in the comments, particularly from the C-suites of micro- and small-cap companies. But there are ways for smaller public companies that are exchange listed (or that aspire to be exchange listed) to cost-effectively implement or optimize internal audit functionality and SOX compliance. Here's how.

Adding a Cost-Effective Internal Audit Function

Narrative preparation. Smaller reporting companies may consider limiting written documentation to material financial processes. These documents can often be created in-house. It's a good practice to consider appointing a point person as the gatekeeper of the narrative documents. Once the documents are completed, consider creating a two- or three-person committee to agree on the key controls for each narrative.

Test using in-house staff. Smaller companies may consider testing only key controls annually. When testing those controls, consider using in-house staff that is not responsible for the area being tested. For example, a payroll manager could be tapped to test SOX controls regarding vendor payments. It's often possible to keep testing records on a basic spreadsheet that identifies key financial risks, testing steps, items tested, and results. Depending on the size of the company, maintaining the testing records can involve as few as one or two employees.

Reporting results. Subsequent to testing, don't overcomplicate communicating the results to the board—what controls were tested, what passed, and what failed.

Optimizing 404 Programs

Focus on what's material. The SEC and the Financial Accounting Standards Board are very broad in describing how a smaller company can evaluate what accounts and processes are material. This allows both management and the board some flexibility to set their policy on how to identify material accounts and processes, and when they can change their approach to calculating materiality. Once set, companies should periodically revisit materiality policies to ensure that they suit corporate size and circumstances.

Risk assessment best practices. Once management has created a simple SOX Section 404 materiality policy, it can focus on what the true risks are for a material misstatement. Having a separate SOX 404 risk assessment policy provides guidelines on how management will review SOX 404 risks in conjunction with materiality. A risk assessment policy should also

provide other basic information, including items considered during the annual risk assessment planning process, interim assessments, and final risk scores.

For smaller organizations, it might be daunting to create materiality and risk assessment policies, since calculating materiality and risk scoring aren't routine. Fortunately, there are resources such as AuditNet .org that offer some of these templates for free and sell others for modest fees.

Maintaining an annual review process for these two policies allows an organization to create a flexible SOX 404 process and provide continuity to the management team on how materiality and risk assessment conclusions were reached.

Entity-level controls take center stage. Also known as "tone at the top," entity-level controls define an organization's culture. These controls are heavily weighted at smaller public companies because management teams wear multiple hats. Regulators such as the Public Company Accounting Oversight Board (PCAOB), which periodically review, inspect, and report on how well external auditors perform, are indirectly impacting how well management is documenting and testing entity-level controls.

The PCAOB is putting a stronger audit standard on entity-level controls. For example, it gave stricter guidance on how to audit these controls in Staff Audit Practice Alert No. 11, "Considerations for Audits of Internal Control over Financial Reporting." Audit committees should regularly engage in dialogue with management to gauge the efficacy of entity-level controls.

In May, the PCAOB published *Audit Committee Dialogue*, which is the first in a series intended to provide insights from PCAOB inspections of public company auditors that may be helpful to audit committee members in their oversight of external auditors. One of the foci in *Audit Committee Dialogue* is on entity-level controls and how management effectively evaluates its judgment calls and key estimates in their financial statements.

Documenting judgment calls. Smaller organizations with SOX 404 programs that have remained substantially unchanged for several years may benefit from conducting a thorough review of their SOX documentation. For example, many small companies find that their SOX narratives or flowcharts could be consolidated.

Others that are starting from scratch with a SOX 404 program should consider making a short list of five key financial areas and a single information technology document. Having five, hour-long meetings with key stakeholders to discuss how the company develops its financial statements and principle areas of risk regarding misstating financial results is often a cost-effective use of time. These types of meetings serve as a company's SOX 404 documentation creation meeting as well as its process risk assessment meeting.

Here's a list of narratives smaller organizations should consider creating:

- Financial statement close, including equity, debt, and transaction items
- Revenue, accounts receivable, and client maintenance
- Cash disbursements, accounts payable, and vendor management
- Human resources, payroll processing, and employee data management
- Inventory processing or other industry-specific processes
- Information technology process including change management, physical and logical security, and general operations

Peer benchmarking. In school, sports, and even in our own careers we constantly compare ourselves to others. Yet few organizations ever want to compare their SOX 404 programs to peers—or "score" them.

Larger organizations can afford to hire nationally recognized firms to provide guidance on what scoring mechanisms they should use to define the success of their SOX 404 programs. Smaller organizations, on the other hand, usually define a successful SOX 404 program as a simple "pass" from their external or internal audit consultants.

Smaller public companies should strive to provide more than just a single bullet point on the audit committee agenda confirming that the company passed SOX 404. There are several free publications offered annually by firms such as Protiviti and KPMG that share SOX 404 survey results. While most of the survey participants are larger companies, smaller public companies should focus on these key points:

- Quantity of key SOX 404 controls being tested and in what areas
- Internal company cost to perform SOX 404
- Number of hours the management team spends on SOX 404

Smaller organizations needn't spend extensive time analyzing SOX 404 surveys; rather they should consider focusing on one or two studies every year. Audit committees can then weigh the top three areas in each study they would like management to benchmark itself against. Internal compliance isn't one size fits all, so smaller organizations should focus on benchmarking the areas that are most important to their audit committees.

Takeaways

There is no doubt that internal audit and SOX compliance are particularly burdensome for smaller public companies where financial and human resources can be in short supply. That said, cash and dedicated headcount don't always result in fulsome internal controls. Officers and directors either set a tone of profound integrity or they don't. Fortunately, every company can afford to set the right tone.