A SOX2007.com White Paper

"SOX 404 and Small Companies:

A Cost Effective Approach to 2007 Compliance"

Background

The Sarbanes-Oxley Act (SOX) was passed by Congress in July 2002 to address corporate mismanagement and accounting fraud in financial reporting revealed in the rash of scandals involving Enron, WorldCom, and other large companies.

The requirements set forth for SOX compliance apply to all U.S. public companies, foreign filers in U.S. markets, and privately-held companies with public debt.

For many companies one of the most challenging and costly components of SOX compliance is Section 404. Section 404 requires management to assess and demonstrate that it has established and maintained effective internal controls around financial reporting.

This internal assessment must include management's conclusion on the effectiveness of these internal controls. External auditors are then required to provide an independent assessment as to the adequacy of these controls.

All publicly traded companies must comply with Sarbanes-Oxley by the end of their first fiscal year that ends on or after December 15, 2007

For companies with small market capitalizations (or small-cap) of generally $75 million or less, 2007 will be the first year that they are required to be SOX 404 compliant.

The SEC (Securities and Exchange Commission) has recognized the unique challenges small-cap companies face regarding SOX 404 compliance and has extended the compliance dates for these smaller companies. These smaller companies must be compliant by their first fiscal year ending on or after December 15th, 2007.

Cost Effectiveness: One of the Key issues for Small Companies

At present, the compliance requirements of SOX make no distinction between large and small companies. SOX compliance therefore places a much larger relative burden on small companies, which typically have substantially fewer resources and personnel than their larger competitors.

Thus, cost effectiveness becomes one of the key issues for small companies in achieving SOX 404 compliance.

While frequently a favorable strategy might be to delay working on SOX 404 compliance until as late as possible, this strategy has unfavorable consequences of higher risk and increased cost. Instead, small companies should start their compliance work now, instead of waiting until 2007, for the following reasons:

1) **Priorities**

Additional work created for employees takes away from the core priorities and work responsibilities crucial to small companies.

By starting early, the impact on employees from SOX 404 compliance projects will be spread out over a longer period, leaving enough time for employees to perform important day to day business operations.

2) **Delays**

First-time SOX 404 compliance is highly time-intensive and very often ends up being a more lengthy process than expected.

By waiting until it is too late, there may not be time to properly identify risks, establish key controls, evaluate deficiencies and do proper remediation. External auditors may be required to perform extra work that could have been done ahead of time by the company, usually at a much higher cost.

This unnecessary cost can be avoided when companies start the compliance work earlier.

3) **Mistakes**

When key controls are not established and assessed properly due to the time constraints, testing by internal management and/or external auditors will expose deficiencies around these non-effective controls.

The ineffective controls will have to be re-assessed and corrected to meet the SOX 404 compliance requirements. This work can be avoided if the process and controls are established and assessed correctly in the beginning.

A 2005 study by Cornell University found that small firms with greater board independence and stricter internal controls outperformed similarly sized firms with less independence and looser controls.

4) **Expertise**

Companies will have difficulty finding outside help, as many SOX consultants will be heavily engaged in 2007 with late filers.

Most first year filers seek outside expertise from consultants in order to complete their filings. This creates a strain on the knowledgeable SOX consultants on the market and drives up their rates.

By beginning the process early, outside consultants can be found at lower rates and can work more efficiently in the time period required for filing.

Risk-based Approach to SOX 404 Compliance for Small Companies

What is the most cost effective way for small companies to be SOX 404 compliant for the first time by 2007?

The Public Company Accounting Oversight Board (PCAOB) has found that in many cases that companies and auditors are documenting and testing too many processes and controls that are not likely to have any material impact on financial statements.

Most companies have been employing a "bottom-up" approach, which treats every risk equally and applies the same detailed examination to all processes that control these risks. This results in an unnecessarily large number of controls that pose little or no risk in financial misstatement, and in turn increases the costs associated with SOX 404 compliance.

The PCAOB and SEC have urged companies and auditors to employ a "top-down, risk based" approach to SOX 404 instead of the over-detailed, bottom-up assessment. A top-down, risk-based approach is based on the premise that not all accounts, transactions, and risks are equally important.

The COSO's June 2006 "Guidance to Smaller Companies" provides a framework and recommendations to help small companies manage the cost of SOX compliance.

Stepping in to help with the development and adoption of such an approach has been the COSO (the Committee of Sponsoring Organizations of the Treadway Commission), which has developed internal control frameworks that have become the most accepted guidance by most practitioners and regulators.

In June 2006, COSO issued revised guidance specifically targeted for smaller companies in a publication titled "Internal Control over Financial Reporting – Guidance to Smaller Public Companies." COSO's small business recommendations follow the model of a risk-based top-down approach, thereby reducing the number of processes and key controls relied upon by the companies and auditors.

It is almost always cheaper and more efficient to implement a top-down approach, and more effective at controlling risks.

Small companies can employ the following steps to successfully complete SOX 404 compliance using cost effective top-down, risk-based approach.

1) Identify risks

The first step in a top-down, risk based approach is to evaluate the enterprise risks and the company's corresponding controls.

A classic example is an evaluation of how effective the Board of Directors is at providing oversight and direction to the company's management and operations.

By answering questions such as these, the company will be able to evaluate its enterprise risks:

(a) does the Board and/or Audit Committee have a designated 'financial expert';

(b) is an effective audit committee and compensation in place and active in their respective oversight roles;

(c) does the Board have any (or enough) independent directors; and

(d) does the Board approve and ensure communication to employees of a Code of Conduct and ethical behavior expectations.

The next step is to look through financial statements and identify the risks in financial statement line items. These risks will be higher for significant balances, complex transactions, volatile balances, and balances that require significant management input of estimates and judgment.

Critical (i.e., "high risk") financial statement components are good places to start, such as significant accounts and related financial statement assertions. First, ask what could go wrong and where could it go wrong? Each organization has its own specific risks. Senior management and directors in that organization have the expertise to identify their own organization's risk.

2) **Evaluate the identified risks**

After risks are identified, the risks will need to be evaluated according to their potential impact on financial reporting if not properly controlled.

Analysis will need to be made on the significance of impact, as well as well as the likelihood of control failure.

Significant financial risks are those risks that have a more than remote likelihood of causing an error of meaningful magnitude in financial statements. Each company will have its own methodology when evaluating risks.

3) **Determine key controls**

Once financial reporting risks have been identified and evaluated, management must link them to the key controls that mitigate them. Key controls are the processes and/or procedures that a company relies on to control these risks.

An example of a key control is a requirement of a second authorization on a check for an amount over $10,000. Some risks may be effectively contained through procedures at the top of the organization.

This can reduce the number of control activities that need to be evaluated for SOX 404. This is also good time to review and update documentation and evaluate the effectiveness of the control design according to the current environment.

4) **Perform internal testing**

Internal testing of the controls helps management to assess whether the key controls are operating effectively and as designed to minimize risks.

Testing can be as simple as observing a control in operation, or as complex as selecting numerous samples and testing the control in detail.

The testing methodology will depend on the significance of the risks and likelihood of control failure. The person performing the testing should be independent of the operation of the controls being tested, as well as adequately trained and qualified to perform testing.

When the testing is performed by inappropriate personnel, external auditors will not be able to use the tester's work as support for their audit conclusions without having to perform their own independent tests. This will add unnecessary cost to SOX 404 compliance.

Hiring a qualified 3rd party consultant to perform internal testing is a good option for avoiding "self-evaluations".

5) **Remediate deficiencies**

With the results from the internal testing of the key controls, management can assess the effectiveness of the key controls as well as the significance of any deficiencies identified.

Deficiencies need to be evaluated and classified as being one of the following categories from most to least significant:

- Material weakness
- Significant deficiencies
- Deficiencies

Companies are required to publicly disclose material weaknesses. With material weaknesses, management or the external auditor cannot conclude that internal controls over financial reporting are effective. Material weaknesses should become a top priority when management considers remediation.

Even though companies are not required to disclose deficiencies and significant deficiencies, management should consider remediating them. Without remediation, control deficiencies can become more severe over time and eventually become material weaknesses.

For more information on the definition and framework for evaluation of the deficiencies, go to www.theiia.org/download.cfm?file=20326.

A carefully planned "top down, risk-based" SOX 404 compliance approach outlined above can save small companies a significant amount of time and money by using a company-specific approach that eliminates unnecessary work.

An initial top-down, risk based compliance effort can take up 9 months to a year or longer when spreading out the project to minimize employee impact and performing proper risk assessment upfront.

Companies faced with time constraints will be forced to employ a "bottom-up" approach, which is costly with over-detailed work as discussed earlier.

In Conclusion

For small-cap companies facing SOX 404 compliance by 2007, this is the time to start working on budget, project plan, scope, staffing and schedules.

It is the time to ask:

- What is our budget?
- Who is going to lead the compliance effort?
- What is the timetable of the project?
- Are we going to seek outside help?

If the company decides to seek outside assistance, it is imperative to look for a consulting firm with extensive experience in small company SOX 404 compliance.

Look for companies that do not believe in a one-size-fits-all approach for SOX 404 compliance projects. Flexibility is important. Seek consultants that can tailor a SOX 404 compliance approach to fit your company and avoid unnecessary expenses.

About the White Paper Authors – With offices in Austin, Dallas, and a "sister" company in Silicon Valley, Bridgepoint Consulting LLC specializes in consulting with small to mid-market public and private companies. For further information, visit www.Bridgepoint-Consulting.com or call our Austin headquarters at 512/437-7900.