SOX 404 Efficiency Diagnostic

A Business Case for Utilizing the Crowe® Diagnostic Assessment

Sarbanes-Oxley Act Section 404 (SOX 404) mandates that management must assess and report on the effectiveness of a company's internal controls over financial reporting. This mandate also includes an assessment from a company's external auditors attesting to management's internal controls. However, the Securities and Exchange Commission (SEC) approved guidance to streamline SOX 404 compliance efforts, and management should take advantage of this guidance.

Streamlining SOX 404

Crowe Horwath LLP developed a diagnostic assessment to assist management of public companies in evaluating their current approaches to SOX in light of the SEC standards.

The diagnostic process offers two levels of review:

1. A high-level review in a multihour phone discussion covering the most impactful efficiencies; and
2. A more in-depth one-to-three-day on-site review of your company's SOX program.

A Case for Savings

The following business case illustrates an application of the Crowe detailed assessment with a perspective on procedures used as well as some of the common findings.

Crowe spent two days on-site at a $2 billion in revenue manufacturer with more than 20 global business locations, six key locations as defined

by its SOX program, and two data centers deemed SOX-relevant. The company used SAP® software for enterprise resource planning. Crowe engaged in discussions with the SOX process leader to understand the current approach and also reviewed the scoping documentation, entity-level documentation, and examples of transactional and information technology general controls (ITGC) documentation. The analysis included reviewing testing approaches and evidence and examination of the reporting process to key stakeholders.

Crowe's evaluation of the **scoping program** included:

- Determining the use of a "top-down risk-based" approach to SOX compliance versus a "coverage-based" approach;
- Verifying the impact of higher-level/monitoring controls in the evaluation of risks within any given financial statement account; and
- Reviewing if both quantitative and qualitative factors were used in the scoping approach.

Scoping Conclusions

Crowe identified a "coverage-based" scoping approach that covered many accounts, processes, and controls with no potential material impact on the financials. We also noted multiple locations included in the scope based upon coverage where no risk considerations were relevant. Management did reduce key controls in previous rationalization efforts, but this was only based on quantitative materiality considerations and no qualitative risk considerations.

We also noted the scoping approach did not risk-rate business processes based upon a risk rating of the financial statement accounts. Therefore, the level of documentation did not reflect the risk profile and there were no adjustments to the nature, timing, and extent of testing.

As a result of these findings, we recommended significant changes to reduce the scope of their work. We also identified the need for a formal scoping document to explain the quantitative and qualitative approach and results. This document helps determine the significant processes and related areas within the company and establishes a materiality threshold to track material misstatement of the financial statements under SOX 404.

Crowe's evaluation of the **entity-level program** included:

- Determining sufficient use of higher-level monitoring controls and a mix of controls at the entity level and the transaction level; and
- Focusing on whether components of the Committee of Sponsoring Organizations of the Treadway Commission (COSO) framework – including control environment, risk assessment, information and communication, and monitoring – were incorporated into management assessment efforts.

Entity-Level Conclusions

Crowe suggested the company consider controls from different areas of the COSO model based on a heavy use of entity-level controls but no elimination of detailed transactional controls. We also recommended the creation of a formal fraud risk assessment to identify areas in which to mitigate those risks.

Crowe's evaluation of the ITGC program included:

- Evaluating the alignment of control objectives and usage to confirm they were commensurate with the relevant risks; and
- Reviewing the risks and controls documentation to confirm they only address potential material weaknesses and not the lower level of potential significant deficiencies.

Recommended Enhancements Project 35 – 50 Percent Savings

Using the Crowe AS5/SEC Diagnostic Assessment to review scoping, entity-level, transaction- level, and information technology-level controls identified significant opportunities to improve SOX 404 efficiencies while making sure financial reporting risks are adequately addressed.

ITGC Conclusions

Crowe found no clear mapping between ITGC applications and business processes related to SOX. Additionally, the elimination of duplicative or redundant controls could significantly reduce ITGC compliance efforts. Thus, we suggested reducing duplicate documentation for SAP software (10 control sets), Oracle® software (five control sets), and UNIX® software (seven control sets) by focusing on the "technology environment" instead of focusing on "ITGC functional area."

Lastly, vaguely written documentation for the application of standard controls across technologies (SAP, AMAPS, *Siebel*®, Trinity, etc.) contributed to current difficulties in testing.

Crowe's evaluation of the **transaction-level program** included:

- Reviewing the risks, assertions, and controls documentation to confirm they only address material misstatements;
- Reviewing the clarity of the risks, assertions, and controls; and
- Assessing the mix of controls to confirm the efficient use of automated vs. manual controls and a balance of key vs. nonkey controls.

Transaction-Level Conclusions

Crowe identified multiple opportunities to rationalize controls including the reduction of redundant controls to address the same risks and assertions without much additional assurance. For example, the company's month-end financial reporting controls (149 in total for six consolidated entities) had not changed since the program was established in 2004. We also found documentation of "process" activities rather than true "control" activities.

A modification to the nature, timing, and extent of all testing was also recommended to tie each control test to its specific risk profile. Finally, there were opportunities to baseline automated application controls which allows management to test these controls over multiple years instead of testing each year.

Contact Information

If you would like more information regarding a Crowe AS5/SEC Diagnostic Assessment, please contact Vicky Ludema at 800.599.2304 or vicky.ludema@crowehorwath.com.

RISK12105