

risky businesses

Grant Thornton 

Grant Thornton periodical reporting on risk and improvement services for business owners.

Sarbanes-Oxley Update

Many companies see Sarbanes-Oxley ("SOX") as an opportunity to fine tune business processes and implement improvements that will hopefully bring about greater profitability. Per a study by AMR Research in February 2007, it appears that SOX-related costs only comprised 20% of the overall compliance spending of companies with revenues less than \$1 billion. Furthermore, most companies do admit that while the process can be agonising, it typically ends up beneficial to business.

The Securities and Exchange Commission ("SEC") and the Public Company Accounting Oversight Board ("PCAOB") have recently proposed some important changes in order to assist companies with the inevitable assignment of complying with SOX. These changes were brought about due to feedback from management, auditors and the public in order to provide more extensive guidance on how to appropriately audit and conclude on material controls and also to provide more time for qualifying companies.

Key Changes

The changes to Auditing Standard No. 2 (if approved, to become AS No. 5) were proposed in order to replace unclear definitions with new, more easily interpretable ones to be used when evaluating a significant deficiency or a material weakness. Current thought is to establish a "top-down, risk-based" approach to the evaluation of financial controls. This would place more emphasis on management's expertise in identifying risks and their ability to implement the proper procedures and policies in order to prevent them from eventually becoming material misstatements.

It's all in the verbiage!! Will we be the wiser following the revised guidelines? The following is a brief explanation of the proposed changes to AS2's existing verbiage:

- "More than remote likelihood" replaced with "reasonable possibility"
 - The Board has found that auditors and issuers have misunderstood the term and have therefore applied a much lower threshold when evaluating the likelihood of misstatement. The expected result is that this change in language will considerably improve the interpretation of deficiencies.

- Clarity on meaning of material weakness and exclusion of significant deficiency
 - AS No. 2 describes a material weakness as "a significant deficiency, or a combination of significant deficiencies, that result in a more than remote likelihood that a material misstatement of the annual or interim financial statements will not be prevented or detected" and proposed to replace it with "a control deficiency, or combination of control deficiencies." An audit of internal control aims to determine whether or not a material weakness exists - not to identify deficiencies that, combined or alone, are more harmful than a material weakness.
- Remove "more than inconsequential" and replace with "significant"
 - The term "more than inconsequential" has resulted in auditors and companies spending excess time with deficiencies that are potentially not adequately important enough to the overall internal control system. The replacement term "significant" has been defined as "less than material yet important enough to merit attention by those responsible for oversight of the company's financial reporting."

The revised verbiage to AS2 does not necessarily provide for a lighter external audit. The changes do provide much needed clarification to some tricky areas of SOX but auditors probably would not rely on these changes for concerns pertaining to the level of exposure. Many critics of the proposed changes voice concerns that AS5 will not be enough to significantly lower audit costs as they will probably still take a conservative approach, thus requiring ample documentation and higher audit costs. It is suggested that the best remedy to lowering the audit costs would be to provide numerical guidelines, which would leave less room for ambiguity.

AS5 also provides for the elimination of unnecessary procedures during the audit by removing the requirement of analysing the process that management used in its assessment of internal controls and allowing the auditor to reduce procedures and/or evidence.

AS5 would allow for greater reliance on the work of others, such as management testing and/or the internal audit function. The auditor would be expected to use the framework provided to assess the competence and objectivity of others in order to place a greater reliance on that work. It is also expected that this would help break down the wall typically encountered with the integrated audit.

The changes were proposed in December 2006 and an open public forum ensued for comments until 26 February 2007. For Grant Thornton's official response [click here](#) and refer to page 950.

Two new rules were issued by the SEC in late 2006. The first rule affects foreign private issuers that are not large accelerated filers and have extended the deadline to comply with Section 404(b) (auditor's attestation on internal control over financial reporting) until 15 July 2007. The other rule provides smaller companies/non-accelerated filers more time before having to provide management's report on internal control over financial reporting if filing annual report on or after 15 December 2007. For more information regarding datelines [click here](#).

On 4 April, SEC commissioners voted unanimously to approve the recommendations to bring the SEC and PCAOB proposals closer together. Furthermore, the goal is to have final guidance by the beginning of June 2007 in order to be in place for 2007 audits.

Opportunities for companies

We see this as an additional occasion for accelerated and non-accelerated filers to improve on the entity-level controls and the global risk management process in order to decrease compliance costs in the long run.

Companies should also work closely with their external and internal auditors in order to integrate the new guidance into the audit scope with the goal of reducing compliance expenditures and enjoying the benefits of enhanced business risk management, such as better performance and lower key controls.

Non-accelerated filers can use this time to strengthen entity-level controls and the risk management process in order to allow auditors to rely more heavily on management's assessment. This should result in an acceptable amount of key controls and a streamlined testing process.

Revisit the objectivity of the internal audit function in order to ensure that external auditors will be able to rely heavily on their testing, which will reduce costs and duplicate work and further strengthen the benefits of SOX.

How Grant Thornton Can Help

Integral to an organisation's success, an internal audit is a powerful tool, helping to identify voids, shortcomings and inherent risk potential in policies, processes and information technology.

By objectively assessing the management of risks that a company faces, we can assist your internal audit to:

- Understand the current state or risk management and gaps thereon
- Analyse risks using appropriate standards
- Develop findings and recommendations for management and/or the audit committee.

Grant Thornton's specialists can also assist provide you with an efficient and streamlined approach to your SOX compliance.

The new buzz word, Governance Risk and Compliance (GRC)

Governance Risk and Compliance or GRC as it is often referred to, is the new buzz word in the consulting world. Before dismissing this as old wine in a new bottle, it is pertinent to analyse the rationale behind the coining of this new term and the benefits it offers from a management perspective. Globally, and in the light of recent high profile collapses, there has been a distinct shift in the way companies are being measured. Whilst financial performance is still the number one factor, there are a number of other factors relating to the company's governance, maturity of risk management practices and compliance with legislation that are increasingly being used to measure the success of companies/organisations. GRC offers an integrated approach to managing these three components and is, therefore, a suitable method that managements can utilise to improve on their company's performance.

IT systems will form an essential component of any effective plans to address GRC and should, therefore, be included in the overall GRC initiative. Some of the larger IT systems and Enterprise resource Planning packages do possess features that facilitate and enhance the GRC management capabilities of organisations, however, the challenge lies in appropriately designing and implementing these systems or making changes where need be.

GRC includes:

- Governance, to include frameworks, policies and procedures that companies use to demonstrate their adoption of good governance principles
- Maturity of the company's Risk Management Initiatives and
- Management of everyday compliance issues relating to existing and proposed legislations.

Whilst juggling with these aspects, companies have in the past adopted different approaches in managing governance, risk and compliance, however, current trends are for GRC to be evaluated and managed as part of a common framework that relates to the company's strategic business objectives. The implication of such an approach is that organisations do not view GRC as isolated, project-based activities managed as separate functions but are adopting a unified GRC strategy that guides people, standardises processes, and integrates technology to embed GRC at every organisational level. IT systems can play a significant role in addressing the issues faced in managing GRC.

Governance

In the Australian context, recent surveys indicate that good corporate governance is one of the key items or initiatives on the agenda of the boards of directors of most companies. Corporate governance is being viewed as a key result area by most companies and initiatives in this area include:

- Increased visibility of the board's performance
- Assessing board performance, implementing dashboards to measure board achievements and compare these against industry benchmarks
- Developing diagnostic tools to assist in predicting and avoiding failures in corporate governance
- Succession planning for top executives
- Structure and remuneration of directors
- Implementation of frameworks, policies and procedures to facilitate corporate governance
- Institute corporate social responsibility and other ethical practices and
- Instituting an environment that facilitates effective risk management and compliance.

Risk Management

Risk management has always been a key focus area for most companies. Almost all companies (public or private, small, medium and large) implement and use formal risk management procedures to manage their risks. Risk management includes the following:

- Effective risk analysis and risk assessment processes
- Design and implementation of enterprise wide risk management frameworks, policies, plans and procedures
- Continuous improvement of the risk management plans
- Change management to include people, systems, processes and technology to facilitate effective risk management and
- Management reporting of risks.

Risk management plans should include all areas of operations and be aligned with strategic business objectives.

Compliance

The collapse of several large companies combined with advances in technology and the global environment we live in have led to the proliferation of a host of legislations that managements of companies have to comply with while running their companies.

Compliance legislations cut across industry and vary from the routine stock exchange initiated regulations and SOX or SAS70 requirements, to industry specific legislations such as BASEL II, Payment Card Industry Data Security Standards Emissions Management and TREAD.

Compliance plans should include:

- Identifying and then developing an inventory of all compliance requirements that the company is subject to and assisting in building these into existing IT systems
- Design, development and implementation of an effective compliance management plan through effective use of IT
- Change systems, processes and technology to adapt to compliance requirements
- Regular monitoring of compliance and
- Maintenance of a flexible compliance plan that will accommodate new requirements and changes to existing requirements.

How Grant Thornton can help

Grant Thornton's Business Risk Services is able to assist with management initiatives in facilitating GRC by providing the following services:

- Design and assist in implementing customised Corporate Governance plans in existing IT systems
- Review existing Risk Management plans and provide meaningful inputs to assist in streamlining risk management initiatives with business objectives and with industry standards. Assist in implementing and managing automated risk management solutions and
- Assist in carrying out reviews to address compliance requirements such as SOX, SAS70, Privacy Act and BASEL II.

Grant Thornton

For further information please contact:



Shirley Liew
383 Kent Street
Sydney NSW 2000
T 02 8297 2489
F 02 9299 4445
E sliew@gtntsw.com.au



Andrew Rigele
383 Kent Street
Sydney NSW 2000
T 02 8297 2595
F 02 9299 4445
E arigele@gtntsw.com.au

DISCLAIMER

This newsletter is general in nature and its brevity could lead to misrepresentation. No responsibility can be accepted for those who act on its content without first consulting us and obtaining specific advice.

Grant Thornton (NSW) Pty Ltd is an independent business entitled to trade under the name Grant Thornton. Grant Thornton is a trademark owned by Grant Thornton International and used under licence by independent firms and entities throughout the world. Liability limited by a scheme approved under Professional Standards Legislation.

www.grantthornton.com.au