

Making Sarbanes–Oxley 404 work: Reducing cost, increasing effectiveness

Parveen P. Gupta* and Tim Leech

Received: 6th October, 2005

*Lehigh University, 621 Taylor Street, Bethlehem, PA 18015, USA; Tel: +610-758-3443;
E-mail: ppg0@lehigh.edu

Parveen P. Gupta, PhD, MBA, LLB is the Frank L. Magee Distinguished Professor of accounting at Lehigh University. His teaching, research and business advisory activities focus in analysing financial disclosures, corporate governance, Sarbanes–Oxley, risk and control assessment and internal auditing. He has authored numerous research articles and books in these and other related areas.

Tim J. Leech, FCA-CIA, CCSA, CFE is Principal Consultant and Chief Methodology Officer at Paisley Consulting, Mississauga, Canada. Prior to this, he was the founder and CEO of CARD® *decisions*, Inc., a global niche consultancy specialising in risk and control assessment learning systems and software tools. He has recently co-authored a book on Sarbanes–Oxley with Parveen Gupta and Sally Chan.

ABSTRACT

KEYWORDS: *Sarbanes–Oxley Act, Section 302, Section 404, internal control certifications, COSO*

Section 404 of the Sarbanes–Oxley Act of 2002 is, perhaps, one of the shortest sections of the Act but it has generated the most controversy both domestically and internationally. Although no one disagrees with the overall goals of Section 404 — strengthening and tightening controls over financial reporting — there is considerable opposition, and even disagreement among the regulators, on how best to implement the intent of Section 404 in the most cost-effective manner. The opposition to the implementation of Section 404 was so

intense that less than a month after the 15th March, 2005 due date for first-time Securities and Exchange Commission (SEC) accelerated filers, the SEC hosted a Roundtable on 13th April, 2005 to receive feedback on the implementation experiences of the SEC registrants. The urgency to act was also so strong that the SEC, along with the Public Company Accounting Oversight Board (PCAOB), released new guidance in the form of a Staff Statement, on 16th May, 2005, to provide some clarity and more direction to the registrants as well as their external auditors as they prepared for the year-two certification. In spite of this additional clarification, dissatisfaction with the ‘how to do it’ versus the ‘why to do it’ continues to run high.

After briefly discussing the basic requirements imposed by Section 404 of the Sarbanes–Oxley Act of 2002 within the historical context of reporting on internal controls, this paper focuses on identifying and analysing the underlying fundamental problems that are causing the implementation of Section 404 to be so problematic. The authors believe that the SEC registrants and their external auditors will continue to struggle with similar issues even during the year-two certification process unless these fundamental problems are addressed. Massive cost, confusion and disagreements between registrants and their external auditors are only symptoms of the serious underlying problems with the current regulations. The paper concludes with a number of recommendations that, if followed, have the potential to make Section 404 compliance a value-adding activity that will cost-effectively achieve the goal of promoting transparency and accountability in the US capital markets.

INTRODUCTION

On 30th July, 2002, President Bush signed into law the Sarbanes–Oxley Act (or SOX) that includes what he called ‘the most far-reaching reforms of American business practices since the time of Franklin Delano Roosevelt’.¹ The unanimity in both the House and the Senate for this legislation was precipitated by the ‘perfect storm’ brought about by the financial scandals at companies like Enron, HEALTHSOUTH and WorldCom. These scandals were thought to be caused, at least in part, by the lack of reliable internal controls, which, in turn, created an environment in which fraud was more easily perpetrated. Consequently, among other reforms, Sections 302 and 404 of the Sarbanes–Oxley Act not only required firms to certify their quarterly and annual financial statements but also mandated that, along with management’s annual assessment of the internal controls over financial reporting, external auditors must also separately opine on the effectiveness of a company’s system of internal controls.

Consequently, for the first time, companies are required to publicly disclose material internal control deficiencies to the Securities and Exchange Commission (SEC) in their annual Form 10K filings and any material changes in their internal control system in the quarterly SEC filings. To provide guidance to the external auditors on various issues related to opining on the effectiveness of a company’s internal controls over financial reporting, the Public Company Accounting Oversight Board (PCAOB) issued Auditing Standard No. 2 (or AS2) ‘An Audit of Internal Control over Financial Reporting Performed in Conjunction with an Audit of Financial Statements’ on 9th March, 2004.² Since then, reporting on internal controls over financial reporting by the management and assessment of the same by the external auditors has generated extensive debate in both the corporate and auditing communities.

A review of commentaries in the popular business press as well as comments filed with the SEC by the registrants and auditors, based on their first-year implementation experience, suggest that (1) the abnormally high cost of implementing Sections 302 and 404 and (2) the significant confusion in the implementation guidance provided by the Commission, as well as by the PCAOB, are two major concerns of company managements and their external auditors. The Financial Executives Institute (FEI), an advocacy group that represents Corporate America, has been conducting regular surveys to assess the cost of implementation associated with Sections 302 and 404. In its March 2005 survey, which was completed just after the first Section 404 deadline for the accelerated filers, FEI found that companies with an average revenue of \$5bn spent on average \$4.36m in total compliance cost for Section 404.³ Another recent study found that from 2003 to 2004, for a sample of Fortune 1000 companies, the average audit fee increase was \$2.3m.⁴ Although many of these cost numbers are self-reported, even SEC Commissioners acknowledge that:

‘As we enter the second year of the 404 process, however, it is becoming increasingly evident that everyone greatly underestimated the costs. When the SEC first released its implementation rules for 404 we estimated aggregate costs of about \$1.24 billion or \$94,000 per public company . . . Unfortunately, our estimates were not just low, they were incredibly low.’⁵

Similarly, on the issue of confusion, the NASDAQ survey on 2nd March, 2005 found that more than one-third of the respondents felt that their audit teams lacked the necessary expertise to complete the Section 404 certification due to unclear regulatory direction.⁶ These and many other such

reports in the media have raised eyebrows from all corners including comments from the Act's authors that such high costs are totally unjustifiable. They are concerned that the Act's implementation is not following the spirit of the law, rather, adhering to the letter of the law. Increasing backlash from the corporate community and the political pressure on the SEC and the PCAOB during 2004 and the first quarter of 2005 was so powerful that the Commission conducted a day-long roundtable on 13th April, 2005 to hear the concerns of registrants, auditors and the investor community and receive feedback. The stated goal was to improve implementation of the most problematic sections, 302 and 404, for the following fiscal year. Interestingly, the pundits are already starting to predict that compliance with Section 404 in year two is not getting cheaper. In a recent article in *Compliance Week*, Kelly (2005) reports that 'a new survey of public companies indicates that a solid majority of them will struggle through Sarbanes–Oxley compliance in 2005 much as they did in 2004: understaffed, overworked, and awash in a sea of manual controls that require expensive testing and remediation'.⁷

Although the common wisdom is that changes are needed in a number of areas of the SEC regulations and related PCAOB Auditing Standard No. 2 that implement the Sarbanes–Oxley Act to make compliance with the Act more practical and cost-effective, there is no doubt, in principle, even among the critics, that 'the goals of Section 404 — strengthening and tightening controls over financial reporting are laudable'⁸ and the Act was much needed. The majority of the 233 respondents who filed comment letters with the SEC in response to its call for feedback dated 22nd February, 2005 agree⁹ that the premise on which Sections 302 and 404 are based is valid and management ownership of internal controls is absolutely necessary to restore confidence in the integrity of financial information pro-

vided by the companies. There is no doubt that for the first time on a global scale C-suite executives and boards of directors are taking a hard look at their company's corporate financial reporting practices and disclosures. Whether the implementation of these two sections has significantly improved the reliability and usefulness of the accounting disclosures of US registrants is an empirical question that will only be answered with the passage of time.

In this paper, based on the authors' more than 30 years of collective research and consulting experience in the field of risk assessment and control evaluation, and recent experiences in implementing Section 404 with a number of clients, the authors discuss key underlying problems that have made the well-intentioned Sections 302 and 404 of the Act 'villains' of corporations around the globe. The authors also propose some practical recommendations to steer the current practice more to implementing the 'spirit of the law' rather than just complying with the 'letter of the law'. To fully appreciate the importance of Sections 302 and 404 of the Act, however, it is first important to briefly visit the history that led to the enactment of the Sarbanes–Oxley Act of 2002.

BRIEF HISTORICAL PERSPECTIVE

The notion of requiring management to rigorously assess the adequacy and effectiveness of controls over accounting disclosure and report major control deficiencies to the auditors and investors is far from new. It is essentially the same information that was called for in 1978 by the Commission on Auditor's Responsibilities, better known as the Cohen Commission. In the *Summary of Conclusions and Recommendations*, this blue ribbon commission convened by the American Institute of Certified Public Accountants (AICPA) stated that:

'Users of financial information have a legitimate interest in the condition of the

controls over the accounting system and management’s response to the suggestions of the auditor for correction of weaknesses. Those matters should be disclosed in the proposed report by management. It is consistent with the normal responsibilities for financial reporting that primary reporting responsibility be assigned to management, with a report by the auditor on management’s representations. The auditor should report on whether he agrees with management’s description of the company’s controls and should describe material uncorrected weaknesses not disclosed in that report.’¹⁰

Although the Cohen Commission correctly identified real shortcomings in the way financial statement audits were being conducted in the 1970s, unfortunately the auditing profession chose not to address the issues at that time. The recent frauds by companies like Enron and WorldCom finally provoked Congress, which by rapidly enacting the Sarbanes–Oxley Act of 2002 has now put into motion some of the very same key changes to the audit process and management reporting that the Cohen Commission prophetically called for over 25 years ago.

Describing the primary responsibilities that Sections 302 and 404 assign is relatively easy. Management of a company should identify risks that threaten the reliability of the assertions or claims implicit in their financial statements and note disclosures; identify, document and assess the design and operating effectiveness of the controls in place to mitigate those risks; and conclude whether the existing controls constitute an ‘effective’ system of internal controls over financial reporting. Serious deficiencies in internal controls, including what the SEC and PCAOB regulations call ‘significant control deficiencies’ and ‘material control weaknesses’ must be disclosed to the company’s external auditors and the audit committee. Material control weaknesses must also be

reported to the SEC by registrants in periodic filings. Under the current rules, the existence of even one material control weakness precludes management from concluding that it has in place an effective system of internal control over financial reporting. The company’s external auditor is charged with reporting on whether they agree with the conclusions reached by management and whether, in their opinion, the registrant has an effective system of internal control over financial reporting in accordance with an established control framework. The key problem with the current regulations is not that formally and rigorously assessing and reporting on internal controls over financial disclosures does not make sense. What is problematic is the way these regulations have been interpreted and implemented in practice. The next section of the paper identifies six underlying problems that have contributed to the cost and confusion during the year-one implementation of Sections 302 and 404 of the Sarbanes–Oxley Act of 2002.

KEY UNDERLYING PROBLEMS IN IMPLEMENTING SECTIONS 302 AND 404

Based on a review of the 233 comment letters filed with the Commission, in response to the SEC’s call for feedback on implementation experiences with Sections 302 and 404,¹¹ the registrants appear to have two major complaints related to Sections 302 and 404 of the Act: (1) excessive and unnecessary cost of compliance that does not add in a material way to the effectiveness of the internal controls over financial reporting; and (2) widespread confusion in implementing the SEC Final Rules on Sections 302 and 404 and the PCAOB Auditing Standard No. 2 due to the lack of repeatability and measurability of the compliance effort on a sustainable basis. These complaints are more than justified and should be addressed. Based on the authors’ research, however, the complaints about expense and confusion are, in

fact, symptomatic of a number of serious underlying problems that need careful attention and examination if the regulators are serious about implementing the intent of the Sarbanes–Oxley Act of 2002: improving the reliability of financial disclosures and the overall state of governance within Corporate America. Each one of these underlying problems is discussed in detail below.

Presumption that a binary conclusion on the effectiveness of a company’s system of internal control over financial reporting can be objectively reached

A major area for debate in the current regulations is the presumption that the management, as well as the company’s external auditors, can objectively arrive at a binary (pass/fail) conclusion on the effectiveness of a registrant’s system of internal controls over financial reporting. It is understood that management of a company has a vested interest in arriving at a positive conclusion about the effectiveness of its system of internal control over financial reporting. Given the current state of guidance, methodologies and tools, however, it is not possible for two auditing firms to unequivocally conclude, on a consistently repeatable basis, that a registrant has, or does not have, an ‘effective’ system of internal controls over its financial reporting. The authors’ field experience with various clients and the anecdotal evidence from the first year implementation efforts support this assertion. For example, in an Audit Committee Roundtable¹² recently hosted by KPMG as part of its Audit Committee Institute, a number of audit committee members complained that the audit committee had to spend enormous amounts of time mediating the very different positions of two auditing firms when the client had retained the services of one auditing firm to help it comply with Section 404 while the other was acting as its external auditor. Ironically, during year-one implementation, each

one of the Big 4 public accounting firms in hundreds of instances served as a statutory auditor to clients or as ‘adviser’ to clients that were being audited by a different Certified Public Accounting (CPA) firm. Interestingly, these disagreements related to many sub-components of this larger underlying problem, ranging from agreeing on the scope of the testing and related sample size to defining what is or is not a key control to classifying control deficiencies into significant versus material control weaknesses etc.

Concluding whether a registrant does or does not have an effective system of internal control over financial reporting is like concluding whether a registrant has passed or failed a prescribed test. If the criteria for assessing the effectiveness of internal controls over financial reporting were so ‘objective’, and the methodology to conduct such assessments had the characteristics of ‘representational faithfulness’ (which the profession is still trying so hard to achieve in accounting measurements), one would accept the validity of such pass or fail judgments on a registrant’s system of internal controls over financial reporting. Unfortunately, as discussed in more detail in the next subsection, the most dominant control model — COSO 1992 — does not provide much guidance at the ‘operational level’ to enable consistent and repeatable conclusions where there would be a high degree of consensus for the conclusions reached by the management as well as the external auditor when independently evaluating the effectiveness of internal controls over financial reporting.

The authors propose that, if instead of mandating a binary pass or fail conclusion on a registrant’s system of internal controls over financial reporting, the SEC Final Rules required an assessment, for example, similar to the one that is conducted by the Malcolm Baldrige Quality Award (or some other equivalent model) to gauge the extent to which a company has quality programs and systems in place, many of the reported

problems within the implementation phase would be minimised.¹³ Contrary to the spirit of Section 404, the need on the part of the external auditors to defend their binary conclusion (a point estimate instead of a range) beyond the shadow of a doubt, perhaps due to their litigation exposure, is believed to be one of the major drivers of ‘over-auditing’ and consequently the excessive cost of compliance. The current situation in the Section 404 compliance regime is very similar to the situation within the US medical profession where the fear of frivolous lawsuits and second-guessing of the judgments made by health care providers have led many practitioners to over-document the state of the care provided by them to their patients to justify their choice of treatment strategies.

Absence of guidance for company managements on control assessment criteria

Although the binary conclusion requirement, as discussed above, is believed to be the primary driver of over-auditing and consequently a lot of non-value-added costs, the absence of practical and generally accepted control assessment criteria that company managements can use to assess and report on the effectiveness of their systems of internal control over financial reporting has also led to significant confusion on the part of company managements while attempting to interpret and apply the current guidance in this area. Simply put, registrants and their external auditors are struggling with how the control assessments must be done and how much control documentation and testing is enough to arrive at a conclusion whether a company has an ‘effective’ system of internal controls over financial reporting. In its 16th May, 2005 Staff Statement, the Commission acknowledges that ‘overly conservative interpretations of the applicable requirements and a hesitancy on the part of the independent auditor to use professional

judgement in evaluating management’s assessment resulted in many cases in too many controls being identified, documented and tested’.¹⁴

Current rules require that management and auditors assess a company’s system of internal controls over financial reporting against an acceptable control model. Both the SEC and PCAOB reference COSO 1992 as an acceptable control model to guide this work. At the time of its publication, more than 13 years ago, the COSO 1992 framework was certainly a significant positive step in raising awareness of what would be the elements of a good system of internal control. But it is also true that its authors did not anticipate that their ‘conceptual’ model would, one day, serve as a benchmark for company managements to assess and report on the efficacy of their internal controls over financial reporting. Since the COSO 1992 control model is an overall framework, it lacks practical steps and guidance that are so desperately needed to evaluate whether a company has an effective system of internal control over financial reporting. For example, while using the COSO 1992 model, from an operational perspective, how does one determine whether a particular control is a ‘key control’? And what could change in the ‘control arsenal’ of the company that could render this control a non-key control? In a recent speech, delivered to the National Association of State Treasurers, Paul S. Atkins, one of the SEC Commissioners, raises similar operational questions, albeit without explicit reference to the COSO control framework:

‘Are the material weaknesses being reported actually “material”? Are the accounting firms using more or less consistent definitions of “material weakness” across companies and industries? Is the definition of “key internal control” sufficiently clear, or is it too muddled in bureaucratese?’¹⁵

Similarly, what is the threshold on each one of the five COSO criteria below which both the management and the auditor are precluded from concluding that a company has an effective system of internal control over financial reporting?¹⁶ Currently, it is not the evaluation under the COSO 1992 model that provides answers to this question; rather it is the PCAOB Auditing Standard No. 2 that provides the guidance which begs the question whether the registrants are concluding the effectiveness of their system of internal controls in accordance with COSO or simply that the evaluation has been done in accordance with PCAOB Auditing Standard No. 2.

Consequently, in the aftermath of the SOX year-one certification experience, many registrants and external auditors are questioning whether the COSO 1992 model can truly help them in arriving at 'reasonably consistent qualitative and quantitative measurements of a company's internal control' over time. It is widely known that prior to SOX very few internal auditors provided senior management and audit committees with reports on how their organisations sized up against the COSO criteria. Similarly, very few external auditors wrote management letters prior to SOX that made explicit reference to the five COSO elements and how their audit clients stacked up against each one of these elements. The following comments from the NASDAQ 2nd March, 2005 survey illustrate how the COSO 1992 framework's inability led to over-auditing during the year-one implementation of Section 404:

'No consistent approach from the audit firms — each had different definitions and process models for attestation.'

'What constitutes final attestation of the process? Scope of work seems never ending.'

'Since the Big 4 didn't have agreement on a clear standard, no cohesion among them

resulted and they tried to "out do" each other to be safe.'

Power imbalance

The presumption of the intellectual validity of arriving at a binary conclusion on control 'effectiveness', as well as the absence of practical guidance for registrants on generally accepted risk and control assessment criteria, besides contributing to 'over-auditing' on the part of the majority of the external auditors, have also created a significant power imbalance between company managements and their external auditors. This power imbalance has resulted in significant management/auditor conflict and led to a great deal of 'adversarial' and 'unproductive' conflict between management and their auditors, often over relatively minor issues. A review of the 233 comment letters indicates a great deal of dissatisfaction on the part of both the parties based on their year-one implementation experiences.

Currently, the management of a company is required to grade its internal control weaknesses using a three-tier system — control deficiencies, significant control deficiencies and material control weaknesses. Significant deficiencies and material weaknesses must be reported to the company's external auditor and audit committee of the board. Material weaknesses must also be disclosed publicly in reports to the SEC. This obligation to report major control concerns is one of the most important requirements of the Sarbanes-Oxley Act of 2002 because it puts the responsibility for effective internal controls over financial reporting squarely where it really belongs: company management. In spite of this being such an important compliance requirement to conform to Sections 302 and 404, no practical guidance is available to the registrants from the SEC on how companies should grade their control deficiencies. Consequently, the registrants have no choice but to follow the 'back-door' approach which involves using the same

rules that their external auditors are required to follow to help them determine what they should do to complete their Section 404 audit responsibilities. The SEC's stance on this issue, of relegating the task of developing guidance for registrants to the PCAOB, has been interpreted by issuers as a grant of absolute authority to external auditors. This perceived power imbalance has led many registrants to believe they must comply with their external auditors' subjective views on what constitutes 'effective' internal control and initiate improvements in their control structure consistent with their auditor's subjective view at any cost.

Since under the current scenario the management has limited room to disagree with their external auditor's interpretation of Auditing Standard No. 2 (without a high risk of receiving an adverse opinion on their Section 404 report), most feel that they have no choice except to yield to the external auditor's subjective assessment and demands even to the point where, in the opinion of the management, the costs clearly outweigh the benefits of implementing such controls. In essence, the Commission's lack of direct guidance in this area has created a situation where external auditors now possess wide discretion in subjectively assessing whether a client has, or does not have, an 'effective' system of internal control. The consensus view is that this guidance imbalance tilts the scale, unjustifiably so, in favour of the external auditors' subjective views on how much control is enough.

In all fairness to the external auditors, it is important to note that the PCAOB inspectors, using the same subjective methods, will have to 'second-guess' the work done by both management and external auditors. In light of the massive power the PCAOB yields over the very existence of external audit firms, it is only natural that external auditors will work to minimise their 'disciplinary risk' by over-auditing and passing the additional costs incurred to their clients. This

higher 'bargaining power' afforded to the external auditors by virtue of the absence of practical guidance for management and the 'back-door' approach of relying on PCAOB Auditing Standard No. 2 is one of the major causes of dissatisfaction among SEC registrants and also the driver of high costs (via unnecessary auditing) incurred by the registrants during year one of the Section 302 and 404 compliance cycle.

Under the circumstances, the approach taken to date by the external auditor community is completely rational. Given the high level of corporate and personal risk attached to incorrectly certifying that internal accounting controls are 'effective' (a risk that is bound to materialise in a major way in the near future) why would not external auditors spend their client's resources to insure themselves against potential lawsuits? The 16th May, 2005 Staff Statement issued by the SEC was clearly interpreted by many as a 'slap on the wrist' of the external auditing community and a subtle directive by the SEC to the auditors to 'go easy' on the registrants during the second pass. However, the Commission's as well as the PCAOB's unwillingness to make substantive changes in the official guidance on how to reach a defensible conclusion on control 'effectiveness' leaves one wondering whether external auditors will really behave any differently in year two of the Section 302 and 404 compliance cycle. Economics 101 tells one that rational agents always work in their self-interest. Surveys and commentaries in the media are already starting to appear which indicate that complying with Section 404 is not going to be significantly cheaper in year two.¹⁷ Recently, even one of the SEC Commissioners has also acknowledged this conundrum by publicly stating that 'cost reductions for year two of the section 404 process will not approach the 50% reductions on which many had been counting . . . reductions from year one instead be in the neighbourhood of 5–20% range, and I

predict that the reduction will be at the low end of this range'.¹⁸

So, why has the Commission defaulted to the PCAOB for guidance on how a registrant should assess and report on the effectiveness of its internal control system over financial reporting (and how to grade the identified control weaknesses)? As discussed above, it is due to the lack of existence of a 'generally accepted control assessment criteria' that managements can use to guide them as they assess, grade and report on their system of internal control. Had such a set of generally accepted control assessment criteria existed prior to the Sarbanes–Oxley Act of 2002, it would have made perfect sense for the PCAOB to restrict their work to setting auditing standards for external auditors to guide them when evaluating management's process of assessing their system of internal controls against such a 'generally accepted control assessment' criteria and opining on the validity of management's representations (just as external auditors currently opine on the fairness of a company's financial statements).

Too much focus on controls, not enough on risks

Emphasis on examining controls without clear linkage to risks is another driver that is leading to higher costs of compliance and consequently very vocal complaints of 'shareholder value erosion' and 'non-value-added' costs by registrants. The rules as currently drafted lead the companies and their auditors to use a 'process-centric' or 'control-centric' assessment approach to form their conclusions on control effectiveness. This is an approach that focuses heavily on detailed documentation of activities and process flows and testing of hundreds of controls without any explicit consideration of the significance of the underlying risks that the controls should be designed to mitigate.

None of the requirements in the SEC Final Rules¹⁹ or the PCAOB Auditing Standard No. 2 explicitly direct registrants and their auditors to start their assessments by first documenting and assessing the key disclosure risks, including assessing the likelihood and potential consequences, that threaten the reliability of the key assertions implicit in all financial statements and note disclosures. Logically, one can argue that only once the significant risks have been identified and assessed should efforts be made to identify the key controls that are in place to mitigate them. Under the current regulatory system, it is entirely possible for companies to get a clean Section 404(b) opinion from their external auditors without formally documenting and assessing the key risks that threaten the reliability of their specific accounts and note disclosures. It is conceivable that a client may implicitly pay attention to the underlying risks but that is not as robust as testing the effectiveness of controls by explicitly first focusing on the key risks, particularly the risks that are already known to have caused major misstatements.

Consequently, the emphasis on controls to the exclusion of risks has resulted in unnecessarily high costs to the registrants where the focus has frequently been to painstakingly document all processes that feed the accounting and note disclosures and test controls that are often not genuine 'key' controls. Key controls are the controls that are actually capable of mitigating *real* risks that an organisation faces in its unique financial reporting environment and the ones that history tells are really the dominant causes of major financial debacles. More than 70 per cent of the respondents, according to a recent FEI survey,²⁰ support a risk-based audit approach as opposed to the current 'control-centric' approach. What the term 'risk-based audit approach' means to each of these respondents, however, is almost certainly highly variable. Additionally, the focus

on controls to the exclusion of risks has also led to lack of an ‘integrated audit’ during year-one compliance with Section 404. The same survey finds that only 6 per cent of the respondents believed that an integrated audit was conducted by their external auditors during their first-year compliance efforts. Conducting two stand-alone and separate audits — financial statement audit and audit of internal control over financial reporting — was not only a clear violation of the AS2 by the external auditors, but also resulted in management questioning the value added by this massive effort. Comments by Joanne Berkowitz, the chief risk officer at PMI Group Inc., are representative of this growing sentiment, ‘for the money . . . it is somewhat hard to see the value day-to-day. A lot of companies are still struggling to quantify value, and still will be [in year two]’.²¹

Although PCAOB Auditing Standard No. 2 (see paras. 68–70) does imply that external auditors shift their focus from ‘control-centric’ audits to ‘management assertion-centric’ audits, it is unclear that they *must* focus attention on and ensure the real risks to specific accounts and note disclosures are identified before certifying on a client’s system of internal controls. The 16th May, 2005 Staff Statement by the SEC confirms that suspicion by observing that:

‘One reason why too many controls and processes were identified, documented and tested was that in many cases neither a top-down nor a risk-based approach was effectively used. Rather, the assessment became a mechanistic, check-the-box exercise. This was not the goal of the Section 404 rules, and a better way to view the exercise emphasizes the particular risks of individual companies. Indeed, an assessment of internal controls that is too formulaic and/or so detailed as to not allow for a focus on risk may not fulfill the underlying purpose of the requirements.

The desired approach should devote resources to the areas of greatest risk and avoid giving all significant accounts and related controls equal attention without regard to risk.’²²

Based on a review of the 233 comment letters filed with the Commission, in response to the SEC’s call for feedback on implementation experiences with Sections 302 and 404,²³ it is clear that there was a widespread and excessive focus in the external audit and consultant communities on documentation and ‘reperformance’ of numerous control activities irrespective of whether they effectively mitigated the real risks to reliable disclosures. This was also recently confirmed by one of the SEC Commissioners, in a speech delivered on 20th September, 2005: ‘We learned that the internal controls rule and the PCAOB standards were being applied in an overly-prescriptive manner. In May, both the SEC staff and the PCAOB issued statements that were geared towards moving companies and auditors off their granular approach and towards a more risk-based model.’ Thus, it would not be improper to conclude that, perhaps, during the year-one compliance efforts, the ‘top-down or risk-based approach’ was not the primary driver of control documentation, assessment and testing.

Meaning of ‘more than inconsequential’ and ‘more than remote’

It is widely recognised that when compared with the ‘reportable condition’ mind-set (as per SAS No. 60),²⁴ Auditing Standard No. 2 has lowered the threshold for grading and reporting control deficiencies. Management as well as external auditors are struggling to get a handle on what exactly constitutes ‘more than inconsequential’ and ‘more than remote’. Repeatability in reaching the same

conclusion given the same set of circumstances is often missing. Even though the SEC and PCAOB have referred the registrants and the auditors to SFAS No. 5 'Accounting for Contingencies' issued by the Financial Accounting Standards Board (FASB), SEC's Staff Accounting Bulletin No. 99 on 'Materiality', and 'A Framework for Evaluating Control Exceptions and Deficiencies'²⁵ issued by the nine CPA firms for more guidance on how to 'operationalise' these two contentious criteria, the reality, during year one of Section 404 compliance and even afterwards, is that external auditors are documenting and reporting relatively low-level procedural deficiencies as serious control deficiencies. This is true in spite of the fact that external auditors continue to give clean opinions on the reliability of the numbers being reported in hundreds of annual SEC filings even where management and/or the auditor reported 'material' control weaknesses. Although most agree that such low-level procedural deficiencies did not cause Enron and will not stop WorldCom-like debacles going forward, unfortunately, under the current guidance, external auditors have often felt they have no choice except to document and report these relatively low-level control deficiencies. The main reason cited is that it is very difficult, in a litigious culture, to make an argument against the view that a discovered internal control weakness could be 'potentially' more than inconsequential or less than remote (as defined by the PCAOB Auditing Standard No. 2). Additionally, just as determining materiality in a financial statement audit context has historically proven to be a difficult and elusive concept, the 'more than inconsequential' or the 'dollar exposure' dimension of grading and reporting internal control weaknesses is also proving to be much more contentious and more difficult than had been anticipated. Consequently, given (1) the fear of regulatory sanctions, (2) 'second-guessing'²⁶ of auditors' work by the

PCAOB inspectors, (3) the potential for class-action lawsuits, and (4) the absence of clear practical guidance, it is not surprising that external auditors, to protect themselves from any potential challenges in the future, have set materiality thresholds in control assessments to levels of materiality where the costs of debating whether these issues constitute 'material weaknesses' often outweigh the benefits to be derived by the investors from the reported internal control weakness.

Inconsistencies in Section 302/404 wording vis-à-vis Commission's final rules

Following are some inconsistencies between what the Congress intended in Sections 302 and 404 of the Act and what the respective SEC Final Rules suggest.

Quarterly control effectiveness assessments under Section 302

Section 302 applies to both quarterly and annual reports filed by registrants with the SEC. The literal interpretation of the 302 subsections (a)(4) and (a)(5) calls for a full reassessment of control effectiveness by management *four times a year* and reporting of all significant deficiencies and material weaknesses that are discovered each quarter to the audit committee and external auditor. In the Final Rule issued for Section 404, however, the Commission indicated that it would *not require the full quarterly control effectiveness assessments* called for in Section 302. The specific language used by the Commission to alter the intent of Section 302 is as follows:

'After consideration of the comments received, we have decided not to require quarterly evaluations of internal control over financial reporting that are as extensive as the annual evaluation . . . Accordingly, we are adopting amendments that require a company's management, with the participation of the principal executive and financial officers, to evaluate any

change in the company’s internal control that occurred during a fiscal quarter that has materially affected, or is reasonably likely to materially affect, the company’s internal control over financial reporting.’ (See Section C.3 of the Final Rules on Section 404.)²⁷

It is not clear from the above-mentioned wording if the Commission, by waving the requirement for full quarterly assessment of internal controls over financial reporting, also suspended the need to report significant deficiencies and material weaknesses each quarter to the audit committee and external auditor along with the requirement to disclose *new* material weaknesses that come to light in quarterly control effectiveness certifications to the SEC. One could conclude that a newly detected material weakness during a quarter is a material change in control but would one consider it a material change in control even when that condition existed earlier but the registrant only detected its severity and impact during the current quarter? No one knows what the apparent contradictions between the literal wording of the Act and the SEC Final Rules mean in practice today or whether it will require a lawsuit in the future to resolve where exactly the law really stands on quarterly control weakness reporting related issues.

Additionally, the wording in Section 302(a)(4)(D) implies that disclosure of control deficiencies identified by management during their quarterly assessments should commence with the effective date of Section 302. Even though the SEC Final Rule for Section 302 was effective from 29th August, 2002, due to ambiguity surrounding the Commission’s response to FAQ No. 9 on Section 404²⁸ many registrants concluded that they did not need to report known control problems until their first Section 404 reporting date, in spite of their CEOs and CFOs formally confirming in SEC filings

that the company has an ‘effective’ system of disclosure control.

Distinction between disclosure controls and internal controls

The Commission has confirmed that the requirement that management must assess the effectiveness of ‘disclosure controls’ each quarter and report related conclusions was in full force even prior to the Section 404 Round One assessments. ‘Disclosure controls’, according to the Commission, are to be distinguished from the ‘internal controls’ that ensure reliable financial reporting.²⁹ The distinction between disclosure controls and internal control over financial reporting is subtle and difficult to make in practice. From a practical perspective, the problem is that, if each quarter material changes in internal controls over financial reporting must be disclosed and new significant deficiencies and material weaknesses must still be reported under Section 302 to the audit committee and the company’s external auditor, it would only seem logical that the quarterly analysis of disclosure controls must also ensure that there are effective internal control systems over financial reporting in place to accomplish these two requirements. Thus, the key question that remains is, given the SEC requirement to assess ‘disclosure controls’ each quarter, does it also include proactively assessing the internal control systems in place to identify material changes in internal controls each quarter and situations where the conclusion on control effectiveness for Section 404 has proven to be inaccurate or incomplete by the passage of time? For example, surfacing of major problems in the following quarter with the accuracy of financial numbers reported at year-end would call previously reached Section 404 effectiveness conclusions into question. In other words, should such circumstances invoke a full reassessment of the internal control effectiveness of a registrant?³⁰

Quarterly reporting of control deficiencies

At a technical level, the wording in Section 302(a)(5)(A) requires that significant deficiencies in internal controls over financial reporting must be reported to both the audit committee and the company's external auditor. Although it is clear from the wording in the section that the external auditor should be told about any material weaknesses in control, what is not clear from the wording is whether the audit committee should also be told about them — an obvious anomaly in the drafting that appears to run counter to the intent of the Sarbanes–Oxley Act. Although the Final Rule for Section 302 is silent on this issue, the Final Rule for Section 404 clarifies or, perhaps more bluntly, corrects the intent of the Congress in the Act by requiring that both significant deficiencies and material weaknesses should be reported to the company's external auditor and audit committee. What is still open to debate and interpretation, however, is whether this is to happen quarterly or only annually because this clarification comes from the Final Rules for Section 404 and Section 404 applies only to the annual reports required by Section 13(a) or 15(d) of the Securities and Exchange Act of 1934.

Similarly, the other problematic element of Section 302 is the new obligation imposed by the Commission as a substitute for full quarterly reassessment in Section 404 Final Rules to identify 'any change in the company's internal control that occurred during a fiscal quarter that has materially affected, or is reasonably likely to materially affect, the company's internal control over financial reporting' (see p. 18 of Section C.3 of the Section 404 Final Rule). Identifying changes that 'materially affect' internal controls over financial reporting is not the same as identifying new reportable control weaknesses. It can also mean disclosing areas of the internal control system that were considered adequate before but are now much stronger.

Nothing in the Final Rules indicates that only deficiencies should be disclosed. It can also mean identifying information on the current reliability of accounting processes that calls into question conclusions reached at the prior year-end on internal control effectiveness. This is a new SEC-imposed reporting requirement that is adding to the confusion and controversy as registrants deal with their quarterly assessments in the aftermath of their initial Section 404 reporting. Unfortunately, there is no guidance yet available to registrants on how this step should be accomplished, especially on the key issue of what constitutes a 'material change'.³¹ Interestingly, since external auditors are not required to report on the sufficiency of 'material changes' on a quarterly basis, it would be inappropriate to expect any guidance from the PCAOB on this important matter.

RECOMMENDATIONS TO CONSIDER

This section proffers some recommendations that could help avoid many of the dysfunctional consequences that registrants have experienced during their first year of reporting on the effectiveness of internal controls over financial reporting under Sections 302 and 404. These recommendations, without minimising the positive aspects of the Sarbanes–Oxley Act of 2002, strive to align management reporting on internal control with the intent of the law, with an eye on the cost-effectiveness of reporting on internal controls over financial reporting.

Require that registrants and auditors focus on the acceptability of residual risk

As stated in the previous section, since most registrants are using a 'process-centric' or 'control-centric' approach to their Section 302 and 404 compliance efforts, they run a real risk of missing the real risks that have caused or have the potential to cause accounting misstatements within their

environment. To correct this undue emphasis on controls, attention should be paid to developing rules and regulations that would clearly require companies to identify and assess the real and potential risks that threaten reliable accounting disclosures, documenting the controls that mitigate those risks, and putting appropriate systems in place to identify and monitor key performance indicators that provide evidence whether, in fact, the controls are working and producing a real and potential error rate in the financial reporting process that is acceptable to management and the audit committee of the company. Such an approach focuses on the acceptability of the current ‘residual risk status’ to management and the board, not a subjective view of what constitutes an ‘effective’ control system according to the external auditor. Additionally, this approach allows for a focused assessment of control effectiveness given the requirement of an acceptable level of risk, steering both the management and the external auditor away from ‘mindless’ documenting and testing of internal controls to achieve that ever elusive ‘reasonable assurance’.

In light of the external auditor’s other primary task of opining on the financial statements, less risk will always be preferred to more risk if all costs can be passed to clients and a profit margin earned. While focusing on the acceptability of the ‘residual risk status’, external auditors still have the opportunity to modify their audit approach to compensate for weak controls. They can also go even further if they believe controls are seriously inadequate and deny an opinion on the financial statements if they disagree with the acceptability of the residual risk status given by the company management. This orientation would not only reduce costs and non-productive arguments between management and external auditors, but will also provide much needed ‘legitimacy’ to the periodic control assessment process in the eyes of the management as well as lead to

meaningful discussions between the external auditor and the management on what is the appropriate level of residual risk that is associated with the concept of ‘reasonable assurance’. Additionally, the focus on identifying the current residual risk status will force managements to think of financial disclosures as the product of the current control design and that understanding and controlling the error rate in accounting disclosures is as important as producing high-quality products and services for their customers. In other words, in much the same way as management holds itself accountable for ‘operational excellence’ it will now also be accountable for effectively managing its disclosure risk by achieving a certain level of ‘control excellence’.³²

From an operational perspective, under a *true* risk-based approach, specific accounting line item and note disclosures are stated as objectives (eg ensure inventory disclosure is reliable, ensure accounts receivable disclosure is reliable, ensure the legal proceedings note disclosure is reliable, and so on). Users then proceed to document the significant risks that threaten the reliability of those accounts or note disclosures. What the profession has historically called ‘management assertions’ such as existence or occurrence, completeness, rights and obligations, valuation or allocation, and presentation and disclosure actually form the primary basis for these risks (eg a risk to the reliability of inventory disclosure is that it does not even exist). These ‘assertion risks’ must often be customised and supplemented with risks specific to the industry and company. Only after the key assertion risks have been clearly identified and ranked should efforts be made to identify and document the key controls in place (or related compensating controls) to mitigate such risks. Consequently, under this approach it is not necessary to document all activities in all related supporting processes. The concept of ‘key controls’ still remains valid but under this approach it is con-

textualised and grounded in identifying controls that help mitigate the key risks. By definition ‘key controls’ are the controls that mitigate the most significant risks or mitigate risks most efficiently and effectively. The next step in this process is to document information that helps management and external auditors understand and evaluate the current residual risk status of the client. This should include documenting real or potential situations where the current controls are not likely to be effective and carefully tracking the actual errors being produced by the current control design.

Overall, under the ‘risk-based’ approach the real goal will not be to spend excessive amounts of time debating whether controls are or are not effective. Rather it would be to debate whether the current residual risk status including the current error rate produced by the controls in place is acceptable to the management and the audit committee and whether external auditors understand the current residual risks and believe they can still form a defensible conclusion on the reliability of the accounts. In this regard, the external auditor can first look to the extent of audit adjustments identified and proposed by them to the company management in the past. The auditor-determined adjustments constitute the ‘indicator data’ related to process reliability and the current residual risk status. As long as the external auditor is fully aware of the current residual risk status they should be well equipped to determine what additional audit steps they should take or if it is even possible to ‘audit around’ the control problems and form a defensible audit opinion. This approach has the potential to significantly reduce audit risk — the risk of external auditors giving an incorrect opinion on financial disclosures — and justify the need for any additional audit procedures or use of a larger sample size should such an action be needed. Approaching Sections 302 and 404 in this way would help comply with the intent of the law and would also make

audit opinions on internal control more meaningful.

Although the new COSO ERM framework has some promise of being used with a ‘residual risk focus’, unfortunately during the year-one certifications it has seen limited acceptance. The authors’ review of hundreds of Form 10Ks filed with the SEC by the companies that have failed their first 404 certification as well as companies passing it reveals that none of them used the COSO ERM framework to conclude on the effectiveness of their internal controls. Conversations with external auditors as well as with various registrants reveal that there does not appear to be any specific motivation on the part of either to transition to the COSO ERM model. This desire to stick with the older COSO 1992 framework versus the new COSO ERM framework indicates that Section 404 compliance continues to be approached with a ‘control/process-centric’ mind-set as opposed to the ‘risk-centric’ approach. According to the COSO Board, although elements of the COSO 1992 framework are embodied within the COSO ERM framework, the two frameworks will continue to co-exist and any one can be used by a company or an external auditor to opine on the effectiveness of a registrant’s system of internal control as per the requirements of the PCAOB Auditing Standard No. 2. Anecdotal evidence even suggests that some external auditors are actively discouraging their clients from using the COSO ERM framework as a benchmark for Sections 302/404 certifications because of the belief that opining against COSO ERM will increase the total amount of effort (and costs) required to render an opinion on internal control certification. Since currently the ‘talk of the town’ is to reduce the cost of compliance, it appears that the auditing industry is trying to recover the ‘sunk costs’ of the year-one effort by incurring additional costs during the year-two certification effort.

External auditors should audit the process followed by the management to assess and report on residual risk

As an alternative to attempting to independently form a view on control effectiveness, the external auditor should evaluate the risk and control assessment process used by management (ie the reliability of the process in place to identify and report the current residual risk status) and be required by the PCAOB to test the reliability and completeness of the residual risk status information being disclosed (ie substantively verify that the results reported on the current risks being accepted in light of the controls in place are reliable). Any situation detected by the external auditor where the auditor concludes that it is a conscious misstatement of either the control design documentation or control testing results should be immediately classified as a significant deficiency and reported to senior management and the audit committee pursuant to the fraud reporting requirement in Section 302(a)(5)(B). A pattern of conscious misstatements of either control designs or control test results should be classified as a material weakness in the registrant’s control environment that management must report to the SEC. Deficiencies in management’s control design assessment work and control operations testing that are *not* deemed by the external auditor to be conscious acts (ie those linked to skill deficiency and/or coverage) should be graded and reported to management and the audit committee based on their severity and frequency. Major deficiencies should be reported to the SEC. The authors believe that this approach will result in a very significant reduction in the ongoing cost of complying with Sections 302 and 404. Additionally, this approach will reinforce the importance of maintaining reliable control assessment documentation and focus attention on the competence and integrity of management — two key elements to reliable financial disclosures. Under this scenario,

when the external auditor determines that any element of management’s risk and control assessment process is unreliable they should be allowed to do the amount of additional work they consider necessary to independently form an opinion on the registrant’s current internal control effectiveness over financial reporting and to support their opinion on the company’s financial results. The cost of additional work done by the external auditors due to the discovery of material deficiencies in the client’s risk and control assessment process should be disclosed to the audit committee. External auditors should be provided with explicit guidance by the PCAOB to deal with situations where the control deficiencies and/or control assessment process deficiencies are so severe that they cannot or should not provide an opinion on the financial accounts and notes. Moody’s,³³ the credit rating agency, refers to these situations as Category B control deficiencies. These safeguards will deter the auditors from constantly ‘auditing around’ major deficiencies. All three of the major credit rating agencies are now questioning how external auditors can form a positive opinion on the reliability of the accounts and note disclosures when there is documented evidence of severe and pervasive problems in a client’s control environment including integrity and competency related concerns.

Retain the requirement to develop and maintain risk and control documentation

The requirement that companies develop and maintain reliable risk and control analysis and documentation related to internal accounting control disclosures should be maintained. The fact that so many companies had not developed risk and control assessment documentation related to their internal accounting control disclosures prior to the Sarbanes–Oxley Act of 2002 indicates that

potentially thousands of US senior executives (and their counterparts in US corporations overseas) were signing accounting control declarations with limited or, in some cases, no formal risk and control assessment and testing documentation to support their claims. Although the cost of creating risk and control assessment documentation can be significant, particularly in the first year, this element should continue to be mandatory. It is only logical to say that going forward the cost to update this documentation should be relatively modest. Further, the use of appropriate technology platforms to store and maintain risk and control assessment documentation would make this process even less onerous and more integrated with other internal reporting needs of the registrant.

Require companies to put in place a process to update risk and control documentation quarterly

Section 302 of the Act explicitly calls for quarterly representations on control effectiveness and quarterly reporting of significant deficiencies as well as material weaknesses by company managements to external auditors and audit committees. This requirement was modified by the Commission and replaced with a requirement that for quarterly reporting management need not do a full reassessment and, instead, should identify and report only ‘material changes’ in the company’s controls. The requirement that management certify in SEC filings that significant deficiencies and material weaknesses have been reported to the company’s external auditor and audit committee each quarter has been retained, albeit in a somewhat confused state currently. Although the requirement to identify *material changes in control* was proposed by the SEC as a way to reduce Sarbanes–Oxley compliance costs, it has created significant additional confusion and unnecessary costs. Consequently, it is recommended that management be required to certify that they have a process in place to

update their risk and control assessment documentation each quarter, a process to identify new control incidents or events that provide information on actual control effectiveness, and a process to identify and report any new significant deficiencies and/or material weaknesses detected as a result of that update activity and new information that has surfaced on control effectiveness. Quarterly testing to confirm the operation of controls identified in the control design documentation should not be mandatory; however, a company may wish to do testing throughout the year to support its Section 404 control effectiveness certification. Once a company’s first set of control assessment documentation is in place this requirement should not be overly costly.

Provide flexibility to management in determining the level of control testing necessary to support its internal control assessment conclusion

From the first-year Section 404 implementation experience, it is clear that all Big 4 public accounting firms and many of the smaller CPA firms have established minimum control testing frequency requirements. For various reasons (eg fear of litigation, ‘second-guessing’ of the audit process by the PCAOB inspectors etc), these minimum sample sizes are often made ‘mandatory’ for all internal test samples whether tested by management or by their external audit firm, irrespective of the registrant’s state of internal control assessment effectiveness. Rather than external auditors mandating specific control testing frequencies that management must conform to, regardless of the effectiveness of their internal control assessment structure, management should be allowed to determine how much testing of internal controls they believe needs to be done to produce and maintain a complete and reliable risk and control effectiveness assessment process. For example, in

companies where (1) company staff are highly skilled in developing and maintaining reliable control assessment documentation, and (2) those responsible for operating and overseeing the controls are truthful and candid in disclosing any changes in risks, control design and all relevant and necessary information on the actual operation and effectiveness of internal controls (ie the residual risk status), the amount of testing necessary to verify management representations should be significantly lower than that required for companies where the staff responsible for control assessment documentation are poorly trained, lack integrity or cannot be relied upon based on various reasons. If management makes poor decisions on the amount of control testing necessary to produce reliable control effectiveness assessments for Sections 302 and 404, it will reflect in the audit opinion on their assessment process and the conclusions arrived at by their external auditor on the reliability of the assessment and conclusions (ie they will be proven wrong or challenged by the external auditor on the quality of the support for their conclusions). Staff responsible for the operation of the controls identified in the control design documentation should be responsible for confirming that the controls are operated as described and disclosing any control operations exceptions. Any employee or third party acting on behalf of the company who consciously misstates control assessment documentation, including the frequency and execution of a documented control, should be reported to the audit committee. A pattern of such behaviour should result in management having to report a material weakness in their control environment in their SEC filings.

This approach should allow the management to adjust the amount of testing undertaken to confirm the reliability of their control assessment documentation and control status representations. This approach will significantly reduce the overall Sections 302

and 404 compliance costs in companies that make a good effort to produce reliable control effectiveness assessments and maintain a strong control environment. Companies that lack commitment to providing their audit committee, the external auditors and the SEC with reliable control effectiveness assessments will be identified and penalised through additional external audit costs and public visibility on the quality and integrity of their control assessment disclosures.

Provide guidance to management on how to assess and report on control effectiveness

Currently the primary source of guidance for management to prepare and confirm control assessment documentation is PCAOB Auditing Standard No. 2. For reasons described earlier, this is not optimal. The focus of Auditing Standard No. 2 should be on describing the audit standards to be applied by the external auditor to form an opinion on the reliability of management's risk and control effectiveness assessment and financial disclosures. Audit standards written for external auditors do not constitute appropriate and sufficient guidance for use by company management. They should only provide auditors with a basis for auditing the reliability and completeness of management's process and representations just as they audit the reliability and completeness of the income statements and balance sheet produced by management under Generally Accepted Accounting Principles (GAAP). A completely separate source of guidance (similar to Basel II for managing operational risks in banks, Malcolm Baldrige Quality Criteria for assessing quality programmes etc) is needed that would provide practical guidance for management. Clearly written guidance on acceptable methods to identify, grade and report on residual risk status, including identified control deficiencies (ie real or potential situations where plausible risks will not be mitigated) will help reduce

compliance costs, minimise the number of non-productive debates and disagreements between management and external auditors, and firmly establish management's accountability to consistently produce reliable control assessments and financial disclosures.

In this respect, as alluded to earlier in this paper, the biggest hurdle that the COSO 1992 control model must overcome to make it an 'operationally' acceptable risk and control assessment model is the repeatability of assessment results produced using its broad framework. It is recommended that the SEC should give serious consideration to the idea of developing a risk and control assessment framework to aid company managements in complying with the requirements of Sections 302 and 404. In the absence of the SEC action, a professional association (such as the Institute of Management Accountants (IMA) or Financial Executives International (FEI)) representing the management should take the lead in developing such an assessment and reporting framework. Further, since the rest of the world is considering following in US footsteps by considering to enact 'SOX-like' legislation, it might even be better for these organisations to establish an international consortium that would include company representatives, academics and audit practitioners from various interested nations to develop an internationally recognised and generally accepted internal control assessment criteria and guidance. Interestingly, the Turnbull Review Group, established by the UK-based Financial Reporting Council and charged with the goal to revise the original Turnbull Guidance to align it with the Sarbanes–Oxley Act of 2002, rejected the 404 provisions in its 16th June, 2005 consultation paper. The Group concluded that alignment of the Turnbull Guidance with Section 404 of the Sarbanes–Oxley Act will result in an inappropriate model because of the 'broader scope of the Combined Code and Turnbull Guidance . . . [leading to] a focus on compliance rather

than substantive assessment and management of risk, undermining what was seen as one of the main strengths of the Turnbull approach'.³⁴

Provide guidance to registrants on how to report on control deficiencies and related remediation actions

Last but not least important is that the SEC should provide specific guidance to registrants on what specifically they should be disclosing when a material weakness is reported to the SEC in their annual filings. According to a recent FERF study,³⁵ at least in the pre-Section 404 reporting period, the quality and quantity of information being reported on control deficiencies has been generally poor. The authors' review of the filings under Section 404 reveals similar disclosure patterns. Although one of the goals of the Sarbanes–Oxley Act of 2002 is to improve corporate financial reporting by enhancing transparency in the disclosures, the control deficiency disclosures filed with the SEC to date have been ambiguous, unclear and written in 'legalese' rather than for immediate understanding by a reader of the financial statements. More specifically, the filings often lack a clear description of what risks are currently not being mitigated adequately in the opinion of the assurance providers, which account or note disclosures in SEC filings are impacted or at risk of being wrong, which COSO control category is involved and what is the dollar impact of the discovered control deficiency on various financial disclosures. From the perspective of an investor, the control deficiency disclosures often do not say what happened or what went wrong in a clear and understandable way. Similarly, the corrective actions identified often do not clearly describe how the registrant has fixed the problem and why the control deficiency will not be repeated in the future. The authors believe the reason for this ambiguous reporting is due to the 'back door' approach to finding

what is wrong with the internal controls upon discovering an error or a misstatement in an account or note disclosure.

It will be a shame if, after all this effort and cost, investors are left wondering about the state of effectiveness of internal controls a registrant has over its financial reporting or the level of risk associated with the reliability of the external auditor's conclusions on the financial statements. The fact that external auditors appear, at least so far, to be signalling that they believe they can form defensible opinions on the reliability of the accounting disclosures regardless of the severity of the control problems compounds this situation. It is important that the Commission evaluate and monitor registrants' quality of disclosure in this area and the PCAOB inspectors keep the public accounting firms 'on notice' to ensure external auditors demand open and forthright disclosure of material weaknesses, along with sufficient description of the remediation actions from their clients to achieve the ultimate objective of the Act: enhancing trust, faith and confidence in US financial markets.

GOING FORWARD

Overall, the above-mentioned problems and potential solutions suggest that if during the year-two certification effort people are serious about 'complying with the intent' of the law, in a cost-effective manner, the registrants and the auditors need to come together and collectively 'exert' a fundamental shift in the approach that has so far been used to comply with Sections 302 and 404. Both need to move away from the current dominant approach that focuses on documentation and testing of internal controls as an end in itself, to focusing on determining whether the current residual-risk status of a company warrants a clean audit opinion. Implied in this shift is also the notion of clearly understanding that in this process the management and external auditors have two very different roles and responsibilities. Management of a

company is responsible for deciding what level of residual risk is acceptable to it and then faithfully communicating its decisions on 'risk appetite' to its board of directors and shareholders and preparing reliable financial disclosures that communicate to the capital markets the residual risk retained by the entity, while the external auditors' primary responsibility is to determine whether the management representations in the financial statements truthfully communicate the residual status of the entity and whether they can be relied upon to make investment and credit decisions by the financiers of the corporation.

There is no doubt that the Sarbanes–Oxley Act of 2002 is a well-intended and necessary piece of legislation that has, unfortunately, lost its way during its implementation. In the words of Commissioner Paul S. Atkins, 'complaints seem to derive not from the statute itself . . . but center more on the implementation of the PCAOB's Auditing Standard No. 2'.³⁶ Given that the Act aims to enhance information intermediation in US capital markets by holding companies accountable for transparency in their financial disclosures it serves an important purpose. However, the misguided implementation largely spurred by the ambiguous or at times lack of guidance pertaining to one of the most important sections of the Act is threatening to derail a series of valid corporate governance reforms put in place as a result of the Sarbanes–Oxley Act of 2002. It is to be hoped that the year-two certification and reporting on Sections 302 and 404 will yield more positive results both for the US listed companies as well as for their shareholders.

REFERENCES

- 1 Fried, Frank, Harris, Shriver and Jacobson Law Firm (2002), 'Sarbanes–Oxley Act Adds New Corporate Responsibility and Disclosure Requirements and Creates Auditor Oversight Board', legal brief to clients, 2nd August, p. 1, available at <http://>

- www.fhjs.com/cmemos/020802_sarb_corp_resp.pdf.
- 2 The US Securities and Exchange Commission approved AS2 on 17th June, 2004. After several extensions of the SEC Final Rules Implementing Section 404, all companies with market capitalisation of more than \$75m and year-end date of on or after 15th November, 2004, became subject to reporting for the first time under Section 404 of the Sarbanes–Oxley Act of 2002.
 - 3 Of the total \$4.36m in compliance costs, about \$1.34m was spent for internal costs, \$1.72m for external costs and \$1.30m for auditor fees. FEI Press Release, 21st March, 2005.
 - 4 Eldridge, S. W. and Kealey, B. T. (2005) ‘SOX costs: Auditor attestation under Section 404’, unpublished working paper, University of Nebraska at Omaha, June.
 - 5 Atkins, P. S. (2005) ‘Speech by SEC Commissioner: Remarks before the National Association of State Treasurers’, Incline Village, Nevada, 20th September.
 - 6 NASDAQ Issuer Survey: Sarbanes–Oxley Act, 2nd March, 2005, p. 5.
 - 7 Kelly, M. (2005) ‘404 compliance in year two isn’t getting cheaper’, *Compliance Week*, 12th July.
 - 8 Atkins, ref. 5 above.
 - 9 SEC (2005) ‘Commission seeks feedback and announces date of roundtable on implementation of Sarbanes–Oxley internal control provisions’, 2005–20, Washington, DC, 22nd February. Comment letters can be accessed through the following URL: <http://www.sec.gov/news/press.shtml>.
 - 10 AICPA (1978) *The Commission on Auditors Responsibilities: Report, Conclusions and Recommendations*, AICPA, New York, NY, p. xxiii.
 - 11 SEC, ref. 9 above.
 - 12 KPMG, Audit Committee Institute ‘Audit Committee Roundtable’, 3rd June, 2005, Short Hills, NJ.
 - 13 To ascertain the effectiveness of quality programmes at a company, the Malcolm Baldrige Quality Award assigns a score on a number of predetermined dimensions which can be present in a company in varying degrees. The use of the continuous scale not only compensates for the variance in the assessment of two examiners but also presents to the judges (and to other users) a much richer set of information about the effectiveness of quality programmes at a company. This approach also allows one to differentiate whether a company is barely making the grade or is significantly above the baseline. Disclosure of such data on the effectiveness of a company’s system of internal controls over financial reporting would lead companies towards an ‘excellence’ orientation rather than just a ‘compliance’ mind-set.
 - 14 SEC (2005) ‘Staff statement on management’s report on internal control over financial reporting’, 16th May, p. 5.
 - 15 Atkins, ref. 5 above.
 - 16 It is true that the presence of even a single material weakness precludes management as well as auditor from concluding that a registrant has an effective system of internal control over financial reporting. But this presumes that determining whether a control deficiency is or is not a material weakness is a ‘slam dunk’ process. Unfortunately, grading of control weaknesses into a significant control deficiency or a material control weakness is also fraught with many problems as discussed in the section ‘Meaning of “more than inconsequential” and “more than remote”’.
 - 17 Kelly, ref. 7 above, p. 1.
 - 18 Atkins, ref. 5 above.
 - 19 Although, in the 16th May, 2005 Staff Statement issued by the Commission, the SEC admonishes the external auditors for not taking a top-down/risk-based assessment approach, it stops short of mandating such an approach. Furthermore, the Staff Statements are staff’s views rather than official rules adopted by the Commission.
 - 20 Financial Executives International (2005), ‘FEI Special Survey on Sarbanes–Oxley Section 404 Implementation’, Executive Summary, March.
 - 21 Kelly, ref. 7 above.
 - 22 SEC, ref. 14 above, p. 4.
 - 23 SEC, ref. 9 above.

- 24 AICPA (1988) *Statement on Auditing Standards No. 60: Communication of Internal Control Structure Related Matters Noted in an Audit*, AICPA, New York, NY, April.
- 25 Nine CPA Firms (2004) ‘A Framework for Evaluating Control Exceptions and Deficiencies’, Version 3, 20th December.
- 26 In a recent speech, the SEC Commissioner, Paul S. Atkins, also concurs that ‘the biggest problem seems to be the fact that accountants and companies fear being second-guessed’ (Atkins, ref. 5 above).
- 27 SEC, ‘Final Rule: Management’s Reports on Internal Control over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports’, Release Nos. 33-8238, 34-47986, available at <http://www.sec.gov/rules/final/33-8238.htm> 2003.
- 28 Question 9: Is a registrant required to disclose changes or improvements to controls made as a result of preparing for the registrant’s first management report on internal control over financial reporting? Answer: Generally we expect a registrant to make periodic improvements to internal controls and would welcome disclosure of all material changes to controls, whether or not made in advance of the compliance date of the rules under Section 404 of the Sarbanes–Oxley Act. However, we would not object if a registrant did not disclose changes made in preparation for the registrant’s first management report on internal control over financial reporting. However, if the registrant were to identify a material weakness, it should carefully consider whether that fact should be disclosed, as well as changes made in response to the material weakness.
- 29 At this point, it is important to point out that financial statements in and of themselves constitute key disclosures that are made each quarter by all the registrants.
- 30 In a recent study, Glass Lewis and Company, San Francisco, a proxy research firm, found that 94 per cent of the companies that received qualified opinion on the effectiveness of their internal controls under Section 404 had certified that their controls were effective in their most recent quarterly filings under Section 302. This suggests that companies ‘were using a rubber stamp to certify the effectiveness of internal controls prior to SOX 404’. Townsend, L. and Grothe, M. (2005) ‘Control deficiencies—finding financial impurities: Analysis of the 2004 and early 2005 deficiency disclosures’, Glass Lewis and Company, 24th June.
- 31 Informal discussions with the SEC suggest that the Commission is reviewing this concern and potential guidance may be provided in due course.
- 32 In this area, the Basel operational risk reforms in the banking sector and the Australian and New Zealand Risk Management Standard No. 4360 provide a robust framework to learn from.
- 33 Moody’s Investor Service (2004), Global Credit Research, October, New York, NY, special comment by Michael Doss and Gregory Jonas ‘Section 404 reports on internal control: Impact on ratings will depend on nature of material weaknesses’.
- 34 Klien, M. (2005) ‘Turnbull Review rejects 404 provisions, seeks comments’, *Compliance Week*, 16th August. Also see Turnbull Review Group (2005) ‘Review of the Turnbull Guidance on Internal Control: Proposal for Updating the Guidance’, Consultation Paper, 16th June.
- 35 Gupta, P. P. and Leech, T. (2005) ‘Control deficiency reporting: Review and analysis of filings during 2004’, Financial Executives Research Foundation, Florham Park, NJ.
- 36 Atkins, ref. 5 above.