

What additional guidance will you find helpful?

Would additional guidance to management on how to evaluate the effectiveness of a company's internal control over financial reporting be useful?

Yes. The current guidance is totally focused on auditors and it seems at times we are merely trying to comply with auditor's requirements.

Additional guidance would be useful in areas such as:

- Definition of fraud for SOX and guidelines on the level of controls required
- Further clarification on what constitutes 'material' is needed i.t.o. the disclosure of material changes in internal control.
- The link between entity level controls and process level controls and guidelines on how to leverage of the entity level controls to reduce the number of SOX controls.
- Clarification on when general IT controls are SOX controls
- Assessing operating effectiveness of IT application controls

Are there special issues applicable to foreign private issuers that the Commission should consider in developing guidance to management on how to evaluate the effectiveness of a company's internal control over financial reporting? If so, what are these?

Yes there are special issues to consider, please see examples listed below:

- Country issues and local requirements, governance, etc. should be considered. For example, in South Africa, compliance with the King report means that your corporate governance is supposed to be of a high standard and it would be helpful to know how we can effectively integrate this into SOX. If there are conflicts in for example the structure of the Audit Committee it is troublesome to comply with both.
- How to practically comply with SOX in some third world countries where tax legislation changes without government notices and the tracking of legislation changes is almost impossible.
- How do you handle the practicalities of reporting in a big integrated company with various business units consolidating into the company structure? What is the depth of controls to be documented and tested for SOX compliance?
- How to address SOX controls with rotational or shift workers in the case of major plants?

Would additional guidance in the format of a Commission rule be preferable to interpretive guidance? Why or why not?

Interpretative guidance would be more appropriate as we should all have to comply with the Act. The guidance should however not be so prescriptive that it limits the use of management's judgment. It is merely the application that we need guidance on. However, the guidance should be clear as we do not want to have to discuss the interpretation of guidance for hours. Also the guidance should be specific enough that we do not have interpretive differences with external audit and have to then comply with AS2 again.

Getting this balance will not be easy, but we are confident the Commission will provide guidance in the appropriate format.

What types of evaluation approaches have managements of accelerated filers found most effective and efficient in assessing internal control over financial reporting? What approaches have not worked, and why?

We follow a control self assessment approach. All risks, controls and tests have been documented in an electronic document management system. On a quarterly basis controls throughout the business are tested. Depending on how frequent the controls are exercised, the controls are either tested on a quarterly, six-monthly or annual basis. All controls with control frequencies of daily, weekly, monthly, quarterly and recurring are tested quarterly. Financial period closing controls and six monthly controls are tested twice a year and annual and automated controls once a year. We implemented a cascading certification model and accountability and sign off starts with the control owner. On a quarterly basis the process owner reviews the documentation and the tests results and documented the results of these reviews electronically. He/she also ensure annual risk assessments are performed. In addition every business unit has a compliance committee that meets on at least a quarterly basis to discuss the SOX compliance status, agree remediation for failed tests, approve changes and evaluate deficiencies. At a group consolidated level all deficiencies are combined, final ratings assigned and the results reported to the Audit Committee.

Why have the majority of companies who have completed an assessment, domestic and foreign, selected the COSO framework rather than one of the other frameworks available, such as the Turnbull Report? Is it due to a lack of awareness, knowledge, training, pressure from auditors, or some other reason? Would companies benefit from the development of additional frameworks?

Combination of the above. In opting for a different framework the differences would have had to be addressed and the auditors convinced that the selected framework is sufficient. Due to the time commitment SOX already required this was the best framework to use for the reason mentioned above as well as the fact that some parties were already familiar with eh COSO framework.

We would not really benefit from the development of additional frameworks.

We also seek input on the appropriate role of outside auditors in connection with the management assessment required by Section 404(a) of Sarbanes-Oxley, and on the manner in which outside auditors provide the attestation required by Section 404(b). Should possible alternatives to the current approach be considered and if so, what? Would these alternatives provide investors with similar benefits without the same level of cost? How would these alternatives work?

Alternate procedures should be permitted. For example, if the auditors are performing controls based audit, then they should not have to go and retest management's process as

they are already relying on it. If they follow a substantive approach, then is it necessary to conclude on the control environment?

Consider removing the external auditor's opinion on management's assessment process. Investors need assurance that our internal controls over financial reporting are well designed and operating effectively, this can be obtained without reviewing management's assessment process.

What guidance is needed to help management implement a “top-down, risk-based” approach to identifying risks to reliable financial reporting and the related internal controls?

We need specific guidance on the dept of controls that are needed. How do you follow a “top down” approach in practice? Where do we start and to what level should we go down to? This is particularly important in an entity with multiple locations and business units. If controls are assessed to be adequate at a group level, is this sufficient, or is it necessary to go to the next level and look at each significant business?

Give guidance to what constitutes a significant business unit for SOX purposes.

Does the existing guidance provide sufficient information regarding the identification of controls that address the risks of material misstatement? Would additional guidance on identifying controls that address these risks be helpful?

Existing guidance is comprehensive but covers a much wider range than just internal controls over financial reporting – would like guidance specific to internal controls over financial reporting. Guidance would also be helpful in our exercise to review and reduce our number of SOX controls.

In light of the forthcoming COSO guidance for smaller public companies, what additional guidance is necessary on risk assessment or the identification of controls that address the risks?

Provide further guidance on:

- Fraud controls
- Controls over spreadsheet
- Service organizations and when SAS 70 reports are required

What guidance is needed about the role of entity-level controls in evaluating and assessing the effectiveness of internal control over financial reporting? What specific entity-level control issues should be addressed (e.g., GAAP expertise, the role of the audit committee, using entity-level controls rather than low-level account and transactional controls)?

Guidance required on what should be tested and how should it be tested. The rules in place for the audit committee should be sufficient to cover their requirements and thus it seems superfluous to then have to go and test it.

To what extent can reliance be placed on entity level controls?

And when should one push this down to account and transactional controls? We suggest this should only be applied to significant subsidiaries as already defined by the SEC. GAAP expertise – if an accounting practice committee exists at group level that provides guidance on GAAP treatment of issues as well as accounting policies and these meetings are attended by all business unit financial managers – should GAAP knowledge still be a documented SOX control at a business unit level? Should it still be tested at the business unit level?

Should guidance be given about the appropriateness of and extent to which quantitative and qualitative factors, such as likelihood of an error, should be used when assessing risks and identifying controls for the entity? If so, what factors should be addressed in the guidance?

Yes, clearer definitions are required as well as examples to make the definitions practical.

Should the Commission provide management with guidance about fraud controls? If so, what type of guidance?

Yes.

- Definition of fraud from a SOX perspective should be provided as this is open to interpretation.
- What type of fraud controls are required and to what level of detail?
- Can a significance factor be applied and to what level of management should fraud controls be required?
- Is there a materiality cap on fraud?
- Depth of fraud controls required?

Should guidance be issued to help companies with multiple locations or business units to understand how those affect their risk assessment and control identification activities?

Absolutely - there is always a risk of going too low in the detail because of the multiple locations and businesses.

- Perhaps we should stick to the primary reporting segments only and not have to go much lower than that.
- What is the definition of a testing location?
- What should be done in areas where rotational workers are used? These workers work in plants are work on a two week on two week off schedule. How will their controls be documented and tested? To what extent should hand-over be tested in these cases? Is this too much depth for SOX?
- Sample size guidance

What type of guidance would help explain how entity-level controls can reduce or eliminate the need for testing at the individual account or transaction level? If applicable, please provide specific examples of types of entity-level controls that have been useful in reducing testing elsewhere.

Help on the type of entity level controls that can reduce or eliminate lower level testing is required.

- The extent that management review of processes eliminates detailed testing of process transactions.
- If you have a group-wide accounting practices committee with GAAP experts that give guidance to the group on GAAP interpretation, accounting policies, etc. and the meetings are attended by all financial managers (of the different entities within the group) would this be sufficient to demonstrate US GAAP knowledge? Take into account that this committee is made up of GAAP experts as well as the financial managers of all the business units in the group as well as the financial manager of the group consolidated functions, external audit and the CFO. Why should GAAP knowledge be checked at every business and why should the application of accounting policies be checked at every business unit?

Would guidance on how management's assessment can be based on evidence other than that derived from separate evaluation-type testing of controls, such as on-going monitoring activities, be useful? What are some of the sources of evidence that companies find most useful in ongoing monitoring of control effectiveness? Would guidance be useful about how management's daily interaction with controls can be used to support its assessment?

More guidance on how and what should be documented to show evidence that the control has operated would be wonderful.

- What part of normal management and monitoring functions would be acceptable for SOX? How can evidence be obtained of all these actions?
- A lot of time is being invested in the signing of reconciliations, reports and checklists to prove that these have been reviewed – is this really what the SEC requires? The use of monthly checklists being signed, internal audit reports and fraud registers
- Guidance on what will constitute sufficient appropriate audit evidence in situations where testing and test results are kept on an electronic medium.
- Guidance to the extent of audit evidence that need to be kept as well as the retention period of the documentary evidence would be helpful.
- Guidance should also be provided on the extent of management assessment process – is testing operating effectiveness sufficient or should walkthroughs be performed as well? If so, what frequency? What about testing the adequacy of the control design?

In situations where management determines that separate evaluation-type testing is necessary, what type of additional guidance to assist management in varying the nature and extent of the evaluation procedures supporting its assessment would be helpful?

Guidance on when to use separate evaluations versus relying on ongoing monitoring activities would be helpful.

Would guidance be useful on the timing of management testing of controls and the need to update evidence and conclusions from prior testing to the assessment “as of” date?

Guidance would be useful without being prescriptive as I think each entity must establish what will work best for them. However, acknowledging reliance on controls tested in prior periods or earlier in the year would be useful.

Guidance as to what controls to test when is desperately needed especially the financial period closing controls and the extent that these controls have to be tested and documentary proof retained during the year-end financial reporting process.

What type of guidance would be appropriate regarding the evaluation of identified internal control deficiencies?

- How to determine what should be reported and what is considered inconsequential.
- Can you have an inconsequential weakness in a key control on which reliance is placed?
- The Charts we use are very useful except for the IT chart – this is where much guidance is needed.
- Clearer wording in the charts will be helpful.
- Also guidance in evaluating audit differences will help.
- Guidance on the bases under which deficiencies should be aggregated
- The impact of compensating and/or mitigating controls.
- Guidance on the potential impact of a deficiency as well as the definition of ‘likelihood’.

Would guidance be helpful regarding the definitions of the terms “material weakness” and “significant deficiency”? If so, please explain any issues that should be addressed in the guidance.

These are defined quite well, however more guidance can be provided on how to evaluate the deficiencies in companies with multiple business units and multiple locations. Also, more guidance can be provided on the qualitative factors that have to be considered.

Would guidance be useful on factors that management should consider in determining whether management could conclude that no material weakness in internal control over financial reporting exists despite the discovery of a need to correct a financial statement error as part of the financial statement close process? If so, please explain.

Yes, especially in the case where audit adjustments have resulted in financial statement changes. This guidance should also focus on companies with multiple business units and the evaluation of errors that have been corrected in financial statements or audit adjustments in the different business units prior to consolidation.

Would guidance be useful in addressing the circumstances under which a restatement of previously reported financial information would not lead to the conclusion that a material weakness exists in the company's internal control over financial reporting?

Yes and specifics should be given.

How have companies been able to use technology to gain efficiency in evaluating the effectiveness of internal controls (e.g., by automating the effectiveness testing of automated controls or through benchmarking strategies)?

We use technology to monitor our assessment process, collate deficiencies and track remediation.

Is guidance needed to help companies determine which IT general controls should be tested?

Absolutely – it is very difficult to establish what must be tested and what is important. Guidance on when a general IT control would be a key control should be given.

Were the levels of documentation performed by management in the initial years of completing the assessment beyond what was needed to identify controls for testing? If so, why (e.g., business reasons, auditor required, or unsure about "key" controls)? Would specific guidance help companies avoid this issue in the future? If so, what factors should be considered?

Yes, we documented too many controls due to:

- uncertainty on the definition of a key control
- the lack of guidance from the SEC
- guidance received from external audit firms.

The external auditors are in a difficult position here since the more controls documented and tested, the lower their risk – therefore can they really give an independent opinion?

What guidance is needed about the form, nature, and extent of documentation that management must maintain as evidence for its assessment of risks to financial reporting and control identification?

Are there certain factors to consider in making judgments about the nature and extent of documentation (e.g., entity factors, process, or account complexity factors)? If so, what are they? Definitely guidance on documentation is needed, particularly the nature, extent and retention period.

What guidance is needed about the extent of documentation that management must maintain about its evaluation procedures that support its annual assessment of internal control over financial reporting?

- How long and in what form should the documentation be maintained?
- Should it merely form part of normal documentation or should separate documentation be put in place?
- What constitutes sufficient evidence?
- How long do we retain different types of information?

Is guidance needed about documentation for information technology controls? If so, is guidance needed for both documentation of the controls and documentation of the testing for the assessment?

IT controls are a key area of uncertainty. Guidance should be provided on how these controls should be documented and what should be documented.