Nancy M. Morris, Secretary
Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549-1090

Re: File Number S7-11-06 – Concept Release Concerning Management's Reports on Internal Control Over Financial Reporting

Dear Ms. Morris,

Emerson supports the goals stated by Congress underlying the Sarbanes-Oxley Act of 2002 (the "Act") to increase corporate responsibility, to improve the accuracy and reliability of corporate disclosures and to protect investors by enhancing auditor independence. We appreciate the opportunity to provide feedback related to our experience with Section 404 of the Act ("404").

We are encouraged by the Commission's request for public comment on guidance for management in apparent recognition that there is a need to fix 404 as the costs of compliance have greatly exceeded expectations. Although the costs of 404 have been widely discussed and analyzed, we feel it bears repeating that the Commission's initial estimate of the average cost of complying with 404 was $91,000 per company.[1] A number of studies have indicated a decrease in average compliance costs subsequent to the first year implementation of 404. While these studies differ in the magnitude of the decline, they suggest that companies experienced significant implementation costs, a portion of which were non-recurring. Of greatest concern, however, is the fact that the ongoing costs of compliance continue to greatly exceed the Commission's initial estimates and expectations.

In order to fix something, it is first necessary to understand what is broken. Many have suggested that the higher than expected costs are largely attributable to "deferred maintenance" of management's responsibilities to maintain effective internal control in accordance with the requirements of the Foreign Corrupt Practices Act ("FCPA"). Although deferred maintenance may have contributed to some of the initial implementation costs of 404, this argument does little to explain why the ongoing costs of 404 are as high as they are. We also take exception to this position as it would suggest that companies with consistent track records of clean financial statement audit opinions simply fell into the right numbers. The reality is that most companies had already established effective systems of internal controls that enabled them to produce and report reliable financial statements.

What has changed, however, is the standards with respect to the key elements of effective internal controls, the level of documentation necessary to demonstrate the design and operation of internal controls, and the means by which management must assess the effectiveness of internal control. It is in the interpretation of these new requirements that the costs began to exceed the benefits. We would like to encourage the SEC to redefine the scope of 404 in order to bring it back into alignment with original Congressional intent and SEC expectations. In particular, we believe the SEC should **reinforce through management guidance that the 404 assessment is concerned with the risk of material misstatement.** We hope our comments on the following aspects of **management guidance** will assist the SEC in their efforts:

[1] Securities and Exchange Commission: Management's Report on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports (Release Nos. 33-8238; 34-47986; IC-26068) (June 5, 2003).

- **Form and Extent of Guidance** – Principles-based guidance supported by comprehensive examples of the proper application of management judgment is preferable to inflexible rules. There should be one set of scalable guidance for management of all public companies subject to 404. The concept of materiality has been lost and must be reinforced throughout any forthcoming guidance for management, particularly with respect to the application of a top-down, risk-based approach.
- **Preventative versus Detective Controls** – In practice, the identification of key controls is often performed in the wrong order, resulting in the identification of an excessive number of key controls. A top-down, risk-based approach should consist of identifying detective, monitoring controls prior to preventative, transaction level controls. If monitoring controls sufficiently address the risk of material misstatement, further testing of preventative controls may be unnecessary.
- **Segregation of Duties** – The 404 assessment should be focused on risks that pose a more than remote likelihood of material misstatement. Similar to the above, if the top-down approach suggests that detective, monitoring controls in a given area adequately address the risk of material misstatement then controls surrounding segregation of duties in that area are not key controls and do not need to be tested.
- **IT Controls** – Several IT general controls have been added to the 404 scope without justifying their link to material misstatements in the financial statements and simply because they are deemed to be "pervasive" controls. A top-down approach needs to be utilized to determine which IT controls are key controls from the standpoint of the risk of material misstatements.
- **Multi-location Model –** In a decentralized company with many locations, the risk of a material misstatement is often lower due to diversification. As a result, the baseline level of coverage should be appropriately adjusted lower, with expanded testing only in areas where issues are identified in order to ascertain whether the issues are isolated or attributable to a more significant, systemic issue. This approach is preferred as it would accommodate rotation rather than testing the same locations year after year.

We also propose an **alternative approach to 404**. Much of the redundancy and added cost to 404 is due to the fact that the external auditors are required to formally assess management's assessment process. As a result, we are in a situation where two AS2-level audits are being conducted; one by management and one by the external auditors. The fact is, however, that the investing public is much more concerned with the external auditor's opinion on the effectiveness of internal controls than management's assessment. While we agree that management needs to assess their controls and certify as to their effectiveness, we do not think it is necessary for the external auditor to do a separate formal assessment of management's process nor should management be required to have an AS2-level audit performed by its internal staff in order to provide its assessment. This is redundant and doubles the cost in terms of direct expense and organization disruption with very little or no incremental benefit. As an alternative, the only thing necessary for the external auditor to report with respect to management's assessment is whether the external auditor found a material weakness that management failed to identify. This provides the investing public the information they need: management's assessment as to the effectiveness of their controls, an independent opinion on the effectiveness of internal controls and whether management failed to identify a material weakness.

As noted above, our comments are organized into the following main topics:

- Management Guidance
- Alternative Approach to 404

*   *   *   *

MANAGEMENT GUIDANCE

To help clarify many of our points, we have developed an analysis of the top-down approach summarized in the PCAOB's response to question 38 in the Staff Questions and Answers released on May 16, 2005. This analysis, included in Appendix A, should be read in conjunction with our other comments. As we will attempt to demonstrate, the top-down approach is sound on paper; however, a key element of the top-down approach – the identification of key controls – is often performed using a bottom-up approach that leads to the identification of a number of IT controls and process/transaction level controls that pose only a remote likelihood of a material misstatement.

Form and Extent of Guidance

One of the primary drivers of excessive 404 costs has been a lack of focus on the risk of material misstatement. Any management guidance issued by the Commission should reinforce the concept of materiality throughout, including the identification of significant accounts, the definition of key control, the multi-location approach used by companies with decentralized operations, the determination of what IT controls should be incorporated into the assessment, the consideration given to anti-fraud and safeguarding controls, and the assessment of deficiencies. We agree with the Commission's position that materiality cannot be defined in a strict rule that would apply to all organizations. However, we also recognize that, in practice, thresholds are established by the public accounting profession that often lead to overly conservative scoping, significant accounts determination, and assessment processes. Any forthcoming guidance should provide comprehensive examples of materiality decisions to demonstrate the proper application of management judgment in making such decisions.

As a decentralized company comprised of many small- to medium-sized companies and divisions, we feel that any additional guidance that would be applicable to smaller companies would be equally relevant to us. We are concerned that the development of two different, and potentially divergent, sets of guidance/rules would complicate the assessment process and require additional effort to assimilate. We believe the focus should be on developing scalable guidance that provides for right-sizing the 404 effort. By right-sizing, we refer to guidance that focuses management's efforts in the areas and at the level originally intended by 404.

On the one hand, we are wary of a Commission rule that may impair management's ability to exercise appropriate judgment. On the other hand, we are concerned that high-level guidance will be insufficient to counteract the impact of the "rules" the PCAOB and public accounting firms have developed in their implementation and interpretation of Auditing Standard No. 2 ("AS2"). Given a choice, we would prefer principles-based guidance accompanied by appropriate examples of what should and should not be interpreted from the guidance. Too often, examples demonstrate what should be incorporated based on the overriding principles and little attention is given to providing examples of what may be excluded under certain situations. As a result, the examples are translated into rules as auditors interpret unique circumstances to fall within, or be similar to, the given examples.

Another concern we share with other companies is the development of guidance for management that conflicts with the auditing standards imposed on the external auditors. A hard and fast rule in the auditing standards (the external auditors "should" do such and such) will outweigh a principle in management's guidance. Likewise, the auditing standard should be carefully reviewed to ensure any rules/principles related to the auditor's expectations of what management's assessment should contain are consistent with the guidance provided to management. Along those lines, we agree with the recommendation of the Government Accountability Office in which they recommend the Commission "coordinate with PCAOB to help ensure that section 404-related audit standards and guidance are consistent with any additional guidance applicable to management's assessment of internal control."[2] In fact, we believe it is absolutely critical that the two sets of guidance be aligned.

As an example of where existing management guidance is insufficient and management is largely left to the interpretations of the public accounting firms, we point to the following guidance surrounding general IT controls provided by the SEC: "… the staff expects management to document and test relevant general IT controls in addition to appropriate application-level controls that are designed to ensure the financial information generated from a company's application systems can reasonably be relied upon. For purposes of the Section 404 assessment, the staff would not expect testing of general IT controls that *do not pertain to financial reporting*."[3] (*emphasis* added)

While the principle behind this statement is sound, we are left confused as to how to apply this in practice. We believe it is equally difficult for the external auditor so they resort in most cases to being conservative and including items as key controls even though the link to the financial statements may be obscure. For example, do controls over the physical security of computer hardware pertain to financial reporting (see our example in the IT Controls section)? How about controls to ensure compliance with the anti-bribery provisions of the FCPA? And what about segregation of duties controls that are intended to prevent poor business decisions but do not impact whether the result of those decisions were properly reflected in the financial statements? While such controls are obviously important, it is unclear whether they should be considered within the scope of the 404 assessment.

Suggestions:

- Develop one set of principles-based guidance for management of all public companies subject to 404. Ensure such guidance is scalable and right-sized, with sufficient weight to support the proper application of management judgment. If necessary, provide an addendum of additional considerations for smaller companies. Clearly indicate that although the consideration items are often more prevalent in smaller companies, they should be considered by companies of all sizes.
- Provide comprehensive, balanced examples as a means of encouraging the proper interpretation of the principles-based guidance. For example, comprehensive examples of materiality decisions should be provided to demonstrate the proper application of management judgment in making such decisions.
- Reinforce the concept of materiality throughout any forthcoming guidance, including the identification of significant accounts, the definition of key control, the multi-location approach used by companies with decentralized operations, the determination of what IT controls should be incorporated into the assessment, the consideration given to anti-fraud and safeguarding controls, and the assessment of deficiencies.
- Provide guidance on the scope of internal control over financial reporting ("ICOFR") accompanied by examples/listings of controls, distinguishing between controls that typically would be included and controls that typically would be excluded. For example, an illustrative listing of controls that "do not pertain to financial reporting" would be particularly useful in the areas of IT controls and controls over compliance with laws and regulations.
- Ensure that the PCAOB standards are revised to align with the guidance provided to management.

[2] United States Government Accountability Office Report to the Committee on Small Business and Entrepreneurship, U.S. Senate: Sarbanes-Oxley Act: Consideration of Key Principles Needed in Addressing Implementation for Smaller Public Companies (April 2006) at 58.

[3] Securities and Exchange Commission: Staff Statement on Management's Report on Internal Control Over Financial Reporting (May 16, 2005).

- See Appendix A for additional suggestions surrounding the identification of significant accounts, the concept of relevant assertions, the extent of internal controls documentation, the definition of key control, and the overall sequence of steps for identifying key controls using the top-down approach.

<u>Preventative versus Detective Controls</u>

Several of our comments in this letter suggest that, in many cases, monitoring controls should comprise the majority of key controls for the 404 assessment. We recognize that "…effective internal control over financial reporting often includes a combination of preventative and detective controls…"[4] We also recognize that preventative controls are often more effective in addressing a specific control objective as they typically operate at a higher level of precision than detective controls and, therefore, can be designed (often at a high cost) to prevent misstatements of any size. However, we disagree that the 404 assessment should focus more on preventative controls than on detective controls. While detective controls may operate at a lower level of precision than preventative controls, they are often designed to efficiently operate at a level of precision that will detect any errors or issues that could lead to a material misstatement.

We believe a disproportionate share of the 404 compliance effort has been placed on the control activities component of internal control, which primarily includes process/transaction level controls as well as IT controls (general and application). This component consists primarily of preventative controls whereas the monitoring component of COSO consists almost entirely of detective controls. As we explain in Appendix A, a top-down approach should entail identifying detective, monitoring controls prior to identifying preventative, process/transaction level controls. In practice, the identification of key controls is often performed in reverse, resulting in the identification of an excessive number of key controls. From a 404 perspective, management and the external auditors should perform a risk assessment to "identify controls to test that prevent or detect [material] errors or fraud on a timely basis".[5]

Detective controls are often controls performed regularly by management as part of their ongoing monitoring and oversight. These controls typically are not in place for a specific control objective but instead represent the embedded procedures by which management gets comfortable that the financial statements are fairly stated and understands what is going on in the business. As noted in COSO:

> The internal control system is intertwined with an entity's operating activities and exists for fundamental business reasons. Internal controls are most effective when they are built into the entity's infrastructure and are part of the essence of the enterprise.[6]
>
> Activities that serve to monitor the effectiveness of internal control in the ordinary course of operations are manifold. They include regular management and supervisory activities, comparisons, reconciliations and other routine actions.[7]

The point here is to identify the controls that are embedded in the ongoing management process and capitalize on those controls. For example, the primary intent of a budget to actual review of payroll expense

[4] Public Company Accounting Oversight Board: <u>Auditing Standard No. 2 – An Audit of Internal Control Over Financial Reporting Performed in Conjunction with An Audit of Financial Statements</u> (March 9, 2004) at A-40.

[5] Public Company Accounting Oversight Board: <u>Staff Questions and Answers: Auditing Internal Control Over Financial Reporting</u> (May 16, 2005) at 3. Note that we have inserted the word "material". Please refer to our commentary in Appendix A.

[6] Committee of Sponsoring Organizations of the Treadway Commission: <u>Internal Control – Integrated Framework</u> (May 1994) (hereinafter "COSO") at 14.

[7] COSO at 70.

is to assess whether expenses are in-line with expectations and explain fluctuations as necessary. Although the intent is not to detect fraudulent payroll transactions, detection of material fraud will occur as a result of follow-up on unexpected fluctuations. Likewise, detective controls provide an important deterrent effect that reduces the likelihood that employees will attempt to circumvent the system for their own gain. Finally, as detective controls are often performed in conjunction with the period-end financial reporting process, many of these controls have traditionally been subject to review by the external auditors as part of their financial statement audit. Management should be encouraged to hold out these controls as key controls in order to fight the trend of testing numerous process/transaction level controls that leads to redundancy in the coverage of relevant assertions with inadequate consideration given to the risk of material misstatement.

There are several factors that often lead to the identification of preventative, rather than detective, controls as the key controls in the 404 assessment process. In practice, we have identified three factors that are particularly relevant: level of precision, frequency, and the requirement to address anti-fraud controls.

Level of precision

Level of precision refers to the degree to which a control is designed to prevent or detect misstatements. Preventative controls are often designed to operate at a very high level of precision, such that all misstatements or errors would be expected to be prevented. Detective controls, on the other hand, are often designed to operate at a lower level of precision. Given a choice, management and external auditors often conclude that the control with the higher level of precision is the key control – resulting in the identification of a much higher relative share of preventative controls. The issue is that this decision process often leads to less efficient testing procedures (see Appendix B for an example). As noted above, the 404 assessment is concerned with the risk of material misstatement. A detective control with a lower level of precision may nevertheless be an effective key control if the level of precision is sufficient to detect material misstatements.

Frequency (timeliness)

Another argument for choosing a preventative control over a detective control is that preventative controls operate continuously, whereas detective controls often operate less frequently. As a result, preventative controls prevent errors or misstatements from entering the system, while detective controls are intended to detect errors or misstatements after some period of time. Depending on the frequency with which a particular detective control is performed, it may be more difficult to detect misstatements in a timely manner as the control may only operate monthly, quarterly, or annually. Therefore, it is necessary to evaluate detective controls to assess whether they are performed with sufficient frequency to detect misstatements in a timely manner (i.e., prior to issuance of quarterly or annual financial statements).

Taken together, we believe that the *level of precision* and *frequency* provide a reasonable basis for assessing whether a given detective control is able to detect material misstatements on a timely basis.

Anti-fraud controls

The final argument often cited for choosing preventative controls over detective controls involves the requirement to assess anti-fraud controls and controls over the safeguarding of assets. Preventative controls, such as controls to ensure proper segregation of duties, are often designed with these specific objectives in mind and, therefore, are often automatically incorporated into the 404 assessment. As a result, detective controls may be largely overlooked even though they can detect material misstatements resulting from fraud. An important point here is that regardless of whether a misstatement is attributable to fraud or error, the focus of the 404 assessment is on the probability of material misstatements.

We want to conclude this section by stating that we are not proposing the 404 assessment should be focused entirely on detective controls. In many cases, there may not be adequate detective controls surrounding a particular significant account or relevant assertion. In other cases, it may be more efficient and effective to test preventative controls versus detective controls. The purpose of our comments in this area is to establish that the thought process for identifying key controls requires careful consideration of many factors. Our analysis of the top-down approach in Appendix A and the illustrative example in Appendix B shed additional light on the risks associated with jumping into testing preventative controls. In addition, Appendix D provides a comparison of the benefits and limitations of preventative and detective controls. We recommend the Commission consider this information in any guidance they develop for management.

Suggestions:

- Develop guidance that provides the proper perspective on the consideration of preventative and detective controls, with consideration given to the terms *level of precision* and *frequency*.
- Reinforce that the 404 assessment is concerned with controls to prevent or detect material misstatements, whether caused by error or fraud, on a timely basis.
- Provide a comparison of the benefits and limitations associated with both preventative and detective controls. While this suggestion may seem trivial, it is information like this that will enable management to support the positions they develop by exercising their judgment.

Segregation of Duties

One area where the focus on preventative controls has had a dramatic impact on the 404 assessment process involves segregation of duties ("SOD"). Based on our review of the Final Report of the Advisory Committee on Smaller Public Companies and information surrounding the development of COSO guidance for smaller public companies, we note that this is also an area of great concern to smaller companies. As a large company, we share these concerns and believe that any forthcoming management guidance from the SEC should address SOD in the context of all companies.

We suspect that a major factor contributing to the disproportionate emphasis on SOD is the fact that many companies (including ourselves) and external auditors continue to scope controls based on a concern that significant deficiencies may not be uncovered, instead of focusing their concerns on the possibility of material weaknesses. The example in Appendix B can be used to highlight this risk. Faced with the possibility that misstatements up to 2.5% of pretax earnings may remain undetected by the company's monitoring control, management and the external auditors may conclude that testing SOD controls is necessary for the 404 assessment process. Given the fact that the unaddressed risk (from a 404 assessment perspective) would not typically be considered material, this decision demonstrates a situation where the scope is inappropriately focused on the risk of a significant deficiency, and not the risk of a material weakness.

We are not suggesting that SOD is unimportant. In fact, we believe this is an area for ongoing effort on the part of management and internal audit, particularly due to the operational objectives associated with the safeguarding of assets. However, we believe the 404 assessment process should only be focused on SOD risks that pose a more than remote likelihood of material misstatement. Where these risks do exist, management should identify the controls that are in place to prevent or detect material misstatements on a timely basis, with consideration given to specific SOD controls as well as detective controls performed as part of management's ongoing monitoring processes. The determination of which controls are "key controls" should be based on consideration of the factors we presented in the previous section. For reasons we discuss below and in Appendices A and B, a decision to broadly test for proper SOD without following the top-down approach can result in significant inefficiencies in management's assessment.

There are two relevant categories of fraud that SOD controls are intended to address: fraudulent financial reporting and misappropriation of assets. In our experience, the greatest risk of material misstatement associated with SOD involves the risk of fraudulent financial reporting due to management override. The most important SOD control in this area is ensuring that top financial management does not have the ability to record journal entries as this ability conflicts with their responsibilities for the overall oversight of the financial reporting process. In our experience, there are typically no monitoring controls that can sufficiently mitigate this risk to a point where the risk of a material misstatement is remote.

On the other hand, our experience with the other category of SOD risks (misappropriation of assets) indicates that detective, monitoring controls are often adequate to reduce to a remote likelihood the probability that a material misstatement could occur and remain undetected. As a result, we spend a lot of time assessing SOD controls that would not meet the definition of a key control. We suspect that we are not alone in this regard, and can only assume this is a result of a flaw in the execution of the top-down approach. An analysis of SOD risks within our company would suggest that even those that represent the greatest risk of misappropriation are often adequately mitigated by detective controls that are designed with a level of precision that would detect material misstatements (see Appendix C for a summary of this analysis). Despite this, management and the external auditors continue to test these and many other SOD controls.

Suggestions:

- Provide guidance on the factors to consider when determining which SOD controls are key controls.
- Put SOD into the proper perspective within the context of the 404 assessment process.
- Properly position the identification of SOD controls in the top-down approach (see Appendix A).

IT Controls

Another area that has placed a significant burden on companies' 404 compliance efforts is IT controls. Not so much because the risks involved are nebulous (they are, in fact, fairly intuitive), but more so because of the difficulty in assessing the interaction of other components of internal control (e.g., monitoring) on the likelihood of a material misstatement remaining undetected. The guidance thus far for management and auditors alike is inadequate to bridge the gap between these risks. As a result of insufficient direction, the public accounting firms have interpreted the requirements in this area at the most conservative level, resulting in the identification and testing of an increasing number of IT controls that, in most companies, we suspect pose only a remote likelihood of a material misstatement.

Due to their classification under 404 as pervasive controls, IT controls are often treated similarly to company-level controls. This leads to the conclusion that all other controls are only as effective as the underlying IT controls. While such controls can have a broad impact on the system of internal controls, we believe this classification leads to identifying more IT controls as key than is necessary for purposes of the 404 assessment. In practice, the identification of IT controls often follows a bottom-up approach, not a top-down approach (please refer to steps 1, 6a, and 6d in Appendix A for additional comments).

For example, program changes is one area of IT controls where failure to follow the proper top-down, risk-based approach may lead to excessive, or improperly focused, testing. Program changes are often tested as a common process, without considering whether the program changes pertain to key financial applications and without considering the strength of the company's company-level and monitoring controls. While this approach may provide for the most efficient testing approach in some situations, in other situations significant program changes may be tested in the same manner as less significant ones. This latter approach may lead to ineffective testing of significant program changes and inefficient testing of less significant program changes.

The above discussion is not intended to suggest that program change controls should never be part of the 404 assessment. Rather, it is provided to demonstrate the dangers of taking for granted that any controls should automatically be considered in-scope for 404. If we, as a large company, struggle with this, we certainly understand that smaller companies will find it difficult to strike the right balance. The existing guidance currently available to management (e.g., COBIT) is largely directed at the system of internal controls and not management's 404 assessment. While this guidance is useful, the critical link between IT controls and the risk of material financial statement misstatements is missing. Likewise, we believe the guidance surrounding IT controls provided to the external auditors in the form of AS2 was inadequate. Without substantially more guidance in this area, companies will be forced to continue to rely on the external auditors' interpretations when determining the IT effort to be included within the scope of the 404 assessment.

More specifically, a number of IT controls are included in the 404 scope that do not appear to have a direct correlation to the financial statements or, at a minimum, do not represent key controls. Notably, several IT controls were added to the 404 scope for many companies between Year 1 and Year 2 that may be important controls from an operational standpoint, but do not appear to meet the definition of internal control over financial reporting.

As an example, we added controls surrounding physical security over the Company's computer rooms to the 404 scope in Year 2. While we do not deny the importance of these controls, we find it hard to accept that deficiencies in physical security controls would ever result in a more than remote likelihood of a material misstatement, particularly given the Company's controls over user administration/access and back-up and recovery procedures. Physical access does not impact system access and, therefore, does not impact the possibility of an individual manipulating financial data. The remaining risk, physical theft or destruction of computer hardware, is mitigated by back-up procedures that would minimize the amount of transactional data that would need to be recreated. Likewise, the theft itself would be easily detected, resulting in timely recognition of any losses associated with the theft.

As we cautioned above, we are not intending to imply that no IT controls are relevant to the 404 assessment; however, our intent is to highlight that companies should not jump into including all possible IT controls in their assessment. As the Institute of Internal Auditors ("IIA") puts it "Failure to define the scope of ITGC [IT general controls] can result not only in too much work, but the need to address security and control issues that may have only a very indirect relationship to the possibility of errors in the financial statements."[8] We continue to question why we are testing any IT general controls outside of the areas of backup, access and program changes. Even in those areas, as our first example above illustrated, we question whether we are perhaps including more controls than necessary in the 404 assessment.

Suggestions:

- Provide balanced guidance with respect to the intended scope and assessment of IT controls, including the interaction of other controls that impact the likelihood of a material misstatement.
- Properly position the identification of IT controls in the top-down approach (see Appendix A).

Multi-location Model

The final area that has contributed significantly to excessive compliance costs involves companies with multiple locations. We believe additional guidance is necessary to assist companies in determining the appropriate baseline level of coverage, identifying significant locations, using benchmarking to alternate the locations selected, and avoiding unnecessary duplication of testing efforts by management and the external auditors. Before we address these specific areas, we provide the following comparative summary of our assessment process pre- and post-404:

[8] The Institute of Internal Auditors: Sarbanes-Oxley Section 404: A Guide for Management by Internal Controls Practitioners (hereinafter "IIA Guide for Management") at 36.

In our organization, internal audit performs the majority of the testing procedures for purposes of management's assessment process. The traditional (pre-404) risk model employed by internal audit to develop the annual testing plan included a number of factors to identify the locations that presented the greatest risk. Although size, in terms of selected financial data, was a key criterion in the assessment, the risk model also considered several other criteria, including: recent audit results, geographical location, the nature and extent of any systems changes, turnover in key financial management, and the time since the prior audit. This model provided us the flexibility to "reward" divisions with strong internal controls by rotating these divisions into scope over a three year period. Divisions with weaker systems of internal controls or those that otherwise presented an increased risk were selected more frequently. In the post-404 environment, however, each significant operating unit (at a minimum any unit that contributes 5% of pretax earnings) is subject to almost continuous audits in the form of interim internal control audits performed by internal audit and the external auditor prior to the end of the 3rd quarter, rollforward procedures performed by operating unit management, interim financial statement audits in the 4th quarter, and year-end financial statement audits subsequent to year-end.

Which, we ask, is a better approach and provides more comfort to management and shareholders: a risk model that attains an appropriate baseline level of coverage, is additive to (and not duplicative of) the external auditor's scope, and is really based on risk or a coverage model that involves selecting the largest units over and over again, despite the level of risk involved?

Baseline level of coverage

In a decentralized company such as ours, the risk of a material misstatement is often lower due to the diversification of risk (i.e., multiple units would need to have the same issue with the same directional misstatement). Recognizing this, we believe it would be appropriate to develop a baseline level of coverage and expand testing as necessary in specific areas where identified deficiencies suggest an increased likelihood of a material weakness on an aggregated basis. Accompanied by an appropriate risk assessment based on factors such as those mentioned above, we believe this approach should enable management to set the baseline level of coverage well below the 60 to 75% coverage levels generally used in practice. Under this approach, management could rotate all the locations over a reasonable period of time, say 3 years, while ensuring management's assessment is based on the risk of material misstatement.

Identifying significant locations

A specific area of concern with respect to the multi-location model is the identification of locations that are individually significant. Similar to the approach taken on significant accounts, locations are often selected based on a pre-defined materiality threshold (for example, any location that contributes greater than 5% of pretax earnings). By setting the threshold at this level of materiality, this approach would suggest that there is a more than remote likelihood that the account balances at these locations could be 100% misstated. As this is unlikely, it would seem more reasonable to conclude that the threshold for identifying significant locations should be some level higher than the level of materiality.

Benchmarking

We believe management and external auditors have been inappropriately limited in their ability to apply benchmarking to alternate the locations selected for testing from year to year. The AS2 requirement that each year's audit stands on its own forces the external auditors and, by default, management to visit the same significant locations each year in order to obtain their necessary coverage. Management and external auditors should be provided the flexibility to use benchmarking to determine which locations to visit based on the results of prior year audits and the nature and extent of any changes (or lack thereof) in the business and internal control systems.

Duplication

There is a general expectation that management must perform their testing prior to the external auditors. In practice, this often leads to an expectation that management perform testing at the same locations as the external auditor. As a result, the same locations are often subjected to multiple levels of audits and management testing. This leads to an extreme amount of duplication, with management and the external auditors testing the same controls throughout the year. As an example, our experience suggests the following testing pattern for subjective reserves is not uncommon:

- Internal audit performs interim testing of controls as of the end of the first quarter.
- External audit performs interim testing of controls as of the end of the second quarter.
- Management performs a rollforward assessment of controls as of the end of the third quarter.
- External audit performs a rollforward assessment of controls as of the end of the third quarter.
- External audit performs year-end testing of controls and balances as of year-end.

To eliminate this duplication while expanding overall combined coverage, management should be encouraged to select locations not subject to the external audit and the external auditors should be provided the flexibility under AS2 to accommodate this approach.

Suggestions:

- Provide guidance on coverage, including baseline levels and comprehensive examples of appropriate coverage under different circumstances.
- Provide guidance on the determination of significant locations similar to the guidance required for determining significant accounts.
- Provide guidance on the use of benchmarking (including the consideration of risks, the results of prior audits, and the nature and extent of changes) to vary the locations subject to management's assessment process.
- Provide guidance on methods for minimizing the amount of duplication in 404 locations selected by management and the external auditor. Clearly communicate that there is no expectation that management perform testing at the same locations identified by the external auditor.

ALTERNATIVE APPROACH TO 404

A number of companies and other interested parties have proposed alternatives to the current 404 requirements. In our view, the external auditor's review of management's assessment process does not carry the same weight as the external auditor's independent opinion on the effectiveness of internal controls. Likewise, eliminating management's requirement to assess the effectiveness of internal controls and certify as to their effectiveness would counteract the efforts to reinforce management's accountability for their internal controls. We also believe, however, that investors are most interested in the external auditor opinion on the effectiveness of internal controls. Everything else leads to redundancy and duplication of testing efforts that results in increased costs with little or no incremental benefit.

Smaller public companies continue to receive 404 extensions for the simple reason that the scope of 404 is too great. While we agree the extensions were necessary as the burden on small companies would be too significant under the current 404 regime, we question how investors are being served by these continuing postponements of 404. The best answer is not a different set of rules for small companies, but rather a redefinition of the scope of 404 – one that aligns with original Congressional intent and SEC expectations. We believe investors would receive the same benefits at a much lower cost by eliminating the external auditor's formal assessment of management's assessment process and redefining how management can perform their assessment without a separate AS2-level audit by management.

Eliminate external auditor's formal assessment of management's assessment process

The PCAOB, through AS2, has implemented prescriptive standards that external auditors must follow in performing their assessment of management's assessment process. As commonly recognized, this has led to AS2 becoming the defacto standard for management's assessment process. As a result, there has been a shift from understanding how management monitors the effectiveness of internal controls to critiquing management's assessment process for differences of opinion regarding how the assessment should be performed. Too much time and effort is spent in this area, when it is clear that management is not held to the same rules as the external auditors.

The external auditors need not evaluate how management performed and supported their assessment to issue an independent opinion on the effectiveness of internal controls. Rather, the external audit of the effectiveness of internal control will either validate or invalidate management's assessment. As a result, the external auditor's assessment of management's assessment process can be limited to simply answering one key question: did the auditor identify any material weaknesses not identified by management? If the answer to this question is yes, the auditor's opinion should clearly state that material weaknesses were identified by the auditor and not by management. In this example, investors receive the information they need – the internal controls are not effective and management did not identify the material weaknesses. See Appendix E for a summary of the impact of this proposed approach on the external auditor's opinion and management's 404 certification.

Redefine management's assessment process

In our opinion, management's assessment should be retained; however, this assessment need not represent another AS2-level audit by management. We strongly believe management should be able to make the assertion that its internal controls are effective based on the information that becomes available to management throughout the year from execution of its ongoing financial reporting and control processes (including, but not limited to, monthly financial reporting and analysis, regular budgeting and forecasting activities, and certifications from operating unit management on their financial statements and internal controls), using internal audit to supplement the external audit of internal control by auditing locations selected by management (and which are not audited by the external auditor), and based on the results of past internal and external audits. While management should not be able to base their assessment solely on the results of the external audit, this should be one element management is permitted to consider in making their assessment. As noted above, investors are still served by clearly identifying in the external audit opinion and 404 certification the party that identified any material weaknesses.

We believe this methodology makes practical sense and is a reasonable business approach to testing internal control effectiveness, weighing both the costs and benefits. The analogy we offer is that the current approach is equivalent to requiring management to have internal audit perform an audit of the company's financial statements with scope and coverage sufficient to form an opinion that the financial statements are prepared in accordance with generally accepted accounting principles in order to allow management to make their representations on the financial statements. This is not required today, no one has suggested that this should be required, nor should it be, but yet that is exactly what is required with respect to the assertion by management about internal control effectiveness.

We believe the changes above would lead to significant cost savings while retaining the benefits of 404. Specifically, we believe these changes would provide the following benefits:

- Minimize redundancy in testing. The current process of management performing specific 404 testing of internal controls followed by external auditor testing of the same controls would be minimized.
- Provide for optimal coordination of internal and external audit efforts to maximize reliance and eliminate redundant testing. External auditors would no longer be restricted to relying on internal audit within the

confines of AS2, but rather would be empowered to assess reliance under more flexible standards that permit them to exercise their judgment.
- Reduce the amount of excessive documentation generated solely for the sake of demonstrating the completion of management's assessment process.

In conclusion, we believe this alternative approach would provide for the same level of investor confidence while bringing the cost/benefit relationship back into the proper perspective.

Suggestions:
- Eliminate the external auditor's requirement to perform a formal assessment of management's assessment process.
- Redefine the scope of management's assessment process.

SUMMARY

All companies should be held to the same standard. Although many smaller companies would be unable to bear the costs associated with 404 under the current regime and the Commission's basis for granting extensions is justified, the solution is not to develop a different set of rules for smaller companies. Rather, the solution needs to entail right-sizing the 404 process for all companies. The focus on materiality has been lost and must be restored. Investor confidence can be maintained without a separate AS2-level assessment by management or a formal assessment of management's process by the external auditors.

Should the Commission have any questions regarding our comments, please do not hesitate to contact the undersigned. We appreciate the opportunity to comment on this topic and trust that our comments will be considered in future Commission deliberations.

Sincerely,

Lisa A. Flavin
Vice President – Audit

Appendix A – Analysis of Top-Down Approach

Following is an analysis of the top-down approach summarized by the PCAOB in the Staff Questions and Answers released on May 16, 2005. Information in *italics* represents company commentary on the top-down approach. Information in **bold** represents revisions and additional steps that we believe should be incorporated into the approach.

Step	Top-down Approach Sequence	Comments and Suggestions
1.	Identify, understand, and evaluate the design effectiveness of company-level controls	- *Additional guidance in this area would be beneficial, particularly for companies that have not yet implemented 404.* - *The evaluation of the design effectiveness of company-level controls, and the documentation of that evaluation, are critical to ensuring an effective and efficient assessment. Particular consideration should be given to:* ▪ *Company-level monitoring controls that reduce to a remote likelihood the probability of a material misstatement, whether due to error or fraud, remaining undetected.* ▪ *Senior management understanding of generally accepted accounting principles that are relevant to the business and the communication of accounting policies to the relevant accounting personnel (including those responsible for monitoring the financial statements at lower levels).* ▪ *Controls within the control-environment, particularly those that demonstrate the proper tone at the top and management's expectations with respect to ethics. The latter item is a critical component of management's antifraud programs and controls and often includes controls designed to deter or detect fraud that significantly reduce the likelihood that a <u>material</u> misstatement due to fraud could occur and remain undetected.* ▪ *Management's risk assessment processes, including management's attitudes towards risk.* ▪ *Monitoring activities of internal audit, including internal audit's risk assessment process and the breadth and depth of the annual testing plan.* - *Due to their classification as pervasive controls, IT general controls are often evaluated from a planning standpoint at this step in the sequence. As we explain below, we believe this is the wrong sequence.*
2.	Identify significant accounts, beginning at the financial-statement or disclosure level	- *Despite PCAOB guidance in this area (e.g., the fixed asset example in response to Question 41), this decision often focuses on whether an account is material in relation to some financial statement measure. Public accounting firms and, by default, management are reluctant to conclude that an account with a balance in excess of a certain threshold is not a significant account, regardless of the risk that the account could contain a material misstatement.* - *More guidance is necessary surrounding the incorporation of qualitative factors to identify significant accounts. The guidance should reinforce the concept that an account may be quantitatively large, yet not represent a*

Step	Top-down Approach Sequence	Comments and Suggestions
		significant account if there is only a remote likelihood the account could be materially misstated. - *In addition, guidance should be provided on how to consider the* <u>*relative*</u> *risk of misstatement on the extent of testing required. Significant accounts with a low (yet still more than remote) likelihood of containing material misstatements may be adequately addressed by testing company-level controls whereas significant accounts with a high likelihood of containing material misstatements may require additional testing at the monitoring and process/transaction level.*
3.	Identify the assertions relevant to each significant account	- *Guidance should clarify between "assertions relevant to each significant account" and the* <u>*relevant assertions*</u> *for each significant account. Of all the assertions relevant to a specific significant account, only those where the risk of material misstatement is more than remote should be considered* <u>*relevant assertions*</u>*. For example, existence, completeness and valuation are all assertions that are relevant to a fixed assets account, but existence and completeness may not be a* <u>*relevant assertion*</u> *for fixed assets if the risk of material misstatement associated with these assertions is remote.*
4.	Identify significant processes and major classes of transactions	
5.	Identify the points at which errors or fraud could occur in the process	- *A significant amount of the initial implementation effort is spent in this area. In order to meet the external auditor's expectations, thorough documentation of all ICOFR within the significant processes must be prepared under the premise that the points at which errors or fraud could occur cannot be identified without first fully understanding all of the controls in the process. Although we agree that this provides for the most comprehensive understanding of the overall system of internal controls, we suspect that this will pose a significant burden to smaller companies in the early implementation phases.* - *Additional guidance for companies that have not yet implemented 404 may be necessary to contain the costs associated with this documentation effort. Companies that only document the controls identified in Step 6 may find the external auditors believe this is insufficient.*
6.	Identify controls to test that prevent or detect [**material**] errors or fraud on a timely basis	- *No mention of materiality (this needs to be constantly reinforced throughout the standards and guidance).* - *This is an area where management and the external auditors need more guidance as it is the point where decisions are made that significantly impact the ongoing time and costs associated with evaluating the effectiveness of ICOFR. In our experience, there are many steps within this step that have traditionally been performed using a bottom-up approach, rather than a top-down approach. As a result, we propose 4 additional steps (6.a. through 6.d below.).* - *A definition of key control is required to focus management's assessment on*

Step	Top-down Approach Sequence	Comments and Suggestions
		the controls that could lead to a material weakness if they were to fail. The IIA has suggested the following definition: *“A key control is a control that, if it fails, means there is at least a reasonable likelihood that a material error in the financial statements would not be prevented or detected on a timely basis. In other words, a key control is one that provides reasonable assurance that material errors will be prevented or detected timely.”*[9] *This concept is sound. By providing a definition, management has a basis against which to compare their preliminary listing of key controls. Any controls that do not meet the definition, including anti-fraud and safeguarding controls, would need to be reevaluated. The following “Acid Test” developed by the IIA provides a good starting point for this evaluation:* ▪ *If the key control fails, such that it is not consistently performed as documented, is there more than a remote likelihood of a material error in the financial statements?* ▪ *If the answer to the question above is “No”, is that because there are additional controls (e.g., duplicative or later controls in the process)? Are these controls identified as key controls, and are they effective?* *If controls that appear to be key to address a risk or assertion for a significant account fail the acid test, management should consult with the external auditor to reach agreement that they are not key.*[10] - *In consideration of the above, companies that have already completed a 404 assessment may want to revisit their assessment of deficiencies to determine whether any compensating controls identified are, in fact, key controls. For example, if multiple SOD deficiencies were mitigated by existing monitoring controls, a company should assess whether the monitoring controls are really the key controls.*
6.a.	**Identify monitoring controls (primarily detective) that prevent or detect errors or fraud on a timely basis**	- *Note: Steps 6.a. and 6.b. should typically be performed in parallel to determine the most effective and efficient assessment approach.* - *What is the planned level of precision of the monitoring control?* ▪ *Is the level of precision sufficient to detect material errors and misstatements (including those arising from fraudulent activities)?* ▪ *If not, determine whether controls exist at the control activity level that are designed to prevent material errors and misstatements.* - *What is the frequency with which the monitoring control is performed?* ▪ *Is the frequency sufficient to detect material errors and misstatements in a timely manner (e.g., quarterly)?* ▪ *If not, determine whether controls exist at the control activity level that are designed to prevent material errors and misstatements.*

[9] IIA Guide for Management at 29.
[10] IIA Guide for Management at 32.

Step	Top-down Approach Sequence	Comments and Suggestions
		- *Is the effectiveness of the monitoring control (significantly) dependent on the IT system?* ▪ *Do the individuals performing the control have a basis (other than the adequacy of the IT system) for assessing whether the balance or transaction subject to review may be misstated? Basis may be an understanding of historical experience, knowledge of factors that should impact the account balance, a detailed budget analysis, etc.* ▪ *If yes, consider which IT application controls and general IT controls are absolutely necessary to ensure the effectiveness of the monitoring control.* - *Considering both effectiveness and efficiency, should this control be tested or should a control at the control activity level be tested?*
6.b.	**Identify control activities (primarily preventative) that prevent or detect errors or fraud on a timely basis**	- *The assessment of control activities should be similar to the approach in 6.a. with the overall goal being to identify the control(s) that provide the most effective and efficient approach. If monitoring controls have been identified that provide adequate coverage of the relevant assertions and are sufficient to detect material misstatements on a timely basis, there may be no need to select preventative controls for testing.*
6.c.	**Identify IT application controls (including restricted access and segregation of duties) that are critical to the effectiveness of the controls identified in 6.a. and 6.b.**	- *The SOD controls to be included in the assessment are often identified too early, resulting in SOD controls being identified that are not required to support management's assessment. In practice, we believe this is attributable to the fact that SOD controls are identified prior to, or without consideration of, the assessment of monitoring controls and control activities as we propose in steps 6.a. and 6.b.* - *As we suggest in our comments in the SOD Focus section of our letter, the general approach to SOD is too broad, often based on the assumption that absolute SOD is required across all significant processes. Under the methodology proposed here, only those SOD risks that pose a more than remote likelihood of material misstatement, after consideration of higher-level controls, should be identified as key controls.* - *We are also concerned that an improper focus on restricted access, which focuses on excessive versus inappropriate access, is further clouding the 404 assessment process. We fully agree with the following statement made by the IIA:* *With restricted access, there is a risk of doing more work than is required for Section 404. Although there are excellent business reasons for restricting access to only those functions individuals need to perform their assigned tasks, it is important to remember that only fraud risk that is both material and also misstated in the financials is within the scope for Section 404.*[11]
6.d.	**Identify IT general controls that are**	- *Based on the prior steps, which General IT controls must be evaluated in order to support the evaluation of the controls selected for testing?*

[11] IIA Guide for Management at 38.

Step	Top-down Approach Sequence	Comments and Suggestions
	critical to the effectiveness of the controls in 6.a., 6.b. and 6.c.	- *This step is often performed out of order, resulting in the identification of IT general controls that pose only a remote likelihood of a material misstatement. Please refer to our comments in the IT Controls section of our letter.*
7.	Clearly link individual controls with the significant accounts and assertions to which they relate	- *This part of the process should occur prior to Step 6 (i.e., prior to determining which controls are considered key controls). Otherwise, a company may find late in the process that certain relevant assertions have not been adequately addressed or other assertions may have received more emphasis than necessary.*

Appendix B: Illustrative Example

Assume a company with 1000 employees, annual payroll expense of $50,000,000, and annual pretax earnings of $20,000,000. The company has a preventative control in place to appropriately segregate and restrict access to employee setups and salary/wage changes. In addition, the company has a detective, monitoring control that involves reviewing budget to actual payroll expenses and headcount by department on a monthly basis. The budget to actual reviews would detect misstatements exceeding $500,000 on an annual basis, or 1% of payroll expense and 2.5% of pretax earnings.

Which one of these controls should be considered a key control? Common practice has been to identify the preventative control as the key control for several reasons. First of all, the control would be classified as an anti-fraud, safeguarding control as it is designed to prevent the creation of fictitious employees and, therefore, the misappropriation of cash. Secondly, the planned level of precision of the preventative control is $0 (that is, it would be expected to prevent <u>any</u> fraudulent transactions) versus the planned level of precision of the detective control of $500,000. Finally, it is generally presumed that preventative controls are preferable to detective controls as they operate continuously (i.e., with greater frequency).

Based on this simple analysis, it would appear the choice is clear. However, several additional facts are relevant to the analysis. First of all, the preventative control in this example only addresses the risk of misappropriation. Additional controls must be evaluated in order to address the relevant assertions surrounding payroll, including payroll processing controls. The detective control, on the other hand, is designed to detect any misstatements in excess of $500,000, whether caused by error or fraud. Secondly, as the preventative controls and processing controls are dependent on the underlying payroll application, the applicable IT application controls surrounding payroll (e.g., application-specific access controls and configuration controls over the payroll software) must be evaluated. Finally, consideration must be given to the general IT controls that serve to ensure the payroll application is properly programmed and maintained.

With this additional information, it is no longer clear that the preventative control is the proper approach. Instead of a trade-off between one preventative and one detective control, it now appears the relationship is numerous preventative, processing, and IT controls on the one hand versus one detective control on the other. Furthermore, if any one of the preventative controls is found to be deficient, management may be forced into testing the detective control in order to assess the significance of the deficiency. Faced with this scenario, management should consider whether the detective control is actually the key control.

A couple of key points should be stressed. First of all, **the key control does not necessarily represent the control with the lowest level of precision or the control that is performed more frequently. The important consideration is whether the key control operates with sufficient frequency and at a level of precision that would prevent or <u>timely detect</u> a <u>materia</u>l misstatement.** Secondly, detective controls can be anti-fraud or safeguarding controls. Not only can such controls be designed to detect material fraud, they generally serve as great deterrents of fraud as they demonstrate to employees that their actions are subject to review. Finally, this is an analysis of the controls that should be considered “key controls” for purposes of the 404 assessment – this should not be construed to imply that preventative controls are not required or are unimportant.

In some situations another factor may come in to play when the payroll is processed by an outside service organization. Common practice is to require testing of controls at the service organization and/or a review of a Type II SAS 70 report from the service organization. If nothing else has changed from the assumptions above, the detective control may still be considered the key control. Specifically, if the detective control would timely detect misstatements in excess of $500,000 resulting from processing errors at the service organization, including additional controls in the 404 assessment process is redundant.

Appendix C: Analysis of Common Segregation of Duties (SOD) Risks

Potential SOD Conflict	Risk	Detective Control	Test SOD?
The top financial person at a location has the authority/ability to prepare or input manual journal entries and/or top-side consolidating entries. The individual's ability to initiate transactions conflicts with his/her responsibility for the overall oversight of the financial statements.	Without adequate oversight, the individual has the ability to override the system of internal controls by recording fraudulent entries.	Higher-level monitoring of the location's financial statements may detect some misstatements, but would typically be insufficient to detect entries intended to bring financial performance in-line with expectations. For example, if planned sales were $100M and a fraudulent entry were recorded to increase recorded sales from $95M to $100M, there is a more than remote likelihood that this misstatement would not be detected.	**YES**
An individual with invoice vouching or purchasing capabilities has the ability to add vendors to the vendor master file without a second-level approval.	The individual may be able to create a fictitious vendor, submit a fictitious purchase order, and accept the invoice for payment.	Departmental review of budget versus actual expenditures that is designed with a level of precision that would detect any material misstatements.	**NO**
An individual has the ability to create new customers and issue credit memos (i.e., write-offs).	The individual may create a fictitious customer, submit a sales order and have company product shipped to himself. The individual would then be able to disguise the fraud by issuing a credit to write-off the resulting receivable balance.	Review of credit memo activity that is designed with a level of precision that would detect any material misstatements.	**NO**
An individual has the ability to add employees to the employee master file and process payroll transactions.	The individual may be able to create a fictitious employee and misappropriate cash.	Departmental review of budget versus actual payroll expense that is designed with a level of precision that would detect any material misstatements.	**NO**

Appendix D – Comparison of Preventative Versus Detective Controls

Advantages of Preventative Controls

- Less costly to maintain once properly established
- Less subject to human error
- Operate continuously – not contingent upon person performing the control
- Generally more precise – typically designed to prevent any misstatement or error as they focus on specific objectives

Limitations of Preventative Controls

- System constraints – may be more costly to establish
- Require manual input up-front – if not designed properly, may increase risks rather than minimizing risks
- Inappropriate reliance on system
- Human resource limitations
- Generally limited to one specific objective – narrow scope may require multiple controls

Advantages of Detective (Monitoring) Controls

- Can be designed to address several objectives, including operational, accounting, and fraud
- Provide deterrent effect
- Focus on material misstatements (generally lower than material) provides for more efficient control to establish
- May be less reliant on system if baselined against knowledge of the business
- Often performed as part of management's ongoing monitoring of the business

Limitations of Detective (Monitoring) Controls

- More subject to human error
- Lapses in monitoring or ineffective monitoring can have opposite of deterrent effect (i.e., unscrupulous employees who recognize that monitoring is weak may be more likely to attempt to take advantage of the system and find loopholes in the controls)
- Timing of monitoring may not be sufficient to prevent losses from occurring (although losses could be recorded timely)
- May be difficult to document or otherwise support thoroughness of review and management's thought processes

Appendix E – Alternative Approaches: Audit Opinion and 404 Certification

Results of Management's Assessment and External Audit	External Auditor Opinion	Management 404 Certification
No material weaknesses identified.	Unqualified audit opinion on management's assessment and unqualified opinion on effectiveness of internal control.	Unqualified certification.
Material weaknesses identified by management.	Unqualified audit opinion on management's assessment and adverse opinion on effectiveness of internal controls. Statement included that material weaknesses were identified by management.	Qualified certification - statement included that material weaknesses were identified by management.
Material weaknesses identified by the external auditor.	Adverse audit opinion on management's assessment and adverse opinion on effectiveness of internal controls. Statement included that material weaknesses were identified by the external auditor.	Qualified certification - statement included that material weaknesses were identified by the external auditor.