The Institute of Internal Auditors

May 1, 2006

David A. Richards, CIA
President

Tel: +1 407 937 1200
drichards@theiia.org

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

Response e-mailed to: rule-comments@sec.gov

Re: File Number 4-511 Public Comments on second-year experiences with Implementation of Internal Control Reporting and Auditing Provisions

Dear Ms. Morris:

The Institute of Internal Auditors (The IIA) welcomes the opportunity to comment on our members' second-year experiences with implementation of the Sarbanes-Oxley Act §404, Internal Control Reporting and Auditing Provisions.

Clearly, the first-year implementation of §404 provided many benefits. Most notable were a more engaged system of internal control over financial reporting with active participation by the board, audit committee, and management and a broader understanding of controls by personnel and management throughout the organization. However, it also created many challenges. These included questions regarding cost-benefits; its capacity to significantly impact the confidence of investors; the lack of balanced focus on financial reporting and other business risks; sustainability of the processes; and the redefinition of the relationship between management, internal audit, and external audit.

For this response, The IIA has focused on the evolution of both the benefits and challenges of §404, consolidating comparative experiences of filers that have been through two years of implementation. The following comments have been prepared using the feedback of chief audit executives of 131 organizations who responded to a comprehensive questionnaire (see Attachment A); prominent chief audit executives from Fortune 100 companies who serve on The IIA's Professional Issues Committee; focus groups composed of chief audit executives; and The IIA's Professional Practices staff.

Our overall conclusion is that, although progress has been made, the great majority of the issues identified in year one were still experienced in year two. On the benefits side, our survey results indicate that:

- Management was more successful in ensuring strong corporate governance and quality financial reporting than in year one. More than 75% of respondents believed their organization's §404 efforts have increased the reliability of controls over financial reporting and the vast majority of survey respondents indicated that their organizations have approached §404 with a long-term strategy to achieve sustainability, as opposed to doing the basics just to comply.

Global Headquarters
247 Maitland Avenue
Altamonte Springs, FL
32701-4201 U.S.A.
Tel: +1-407-937-1100
Fax: +1-407-937-1101
www.theiia.org

- The average number of key controls identified by management decreased from 824 to 650, recognizing a more top-down approach by management. 42% of respondents stated that they used this approach in year one, while it was used 75% of the time in year two.

- The relationship between internal and external auditors has migrated from coexistence and coordination to coordination and integration, which indicates an improved risk assessment and audit-planning process.

- 35% of the respondents believed external auditors used their work and the overall audit plan was more effective in year two, up from just 11% in year one.

But, our survey results indicate there are still challenges to implementation:

- When comparing costs from year one to year two, organizations have gained cost efficiencies in their own processes (e.g., creating process documentation, testing key controls) To some degree, these efficiencies should continue to occur into future years. What is noteworthy, however, is that attestation and certification costs associated with SOX remained at the same level of cost for 41% of the respondents, with an additional 7% indicating that attestation costs had increased. In addition, more than 20% of respondents saw an increase in other audit services (e.g., tax) in year two over year one.

- The variance between guidance issued by PCAOB and actual practical experiences seems to be large. For example, in year two, 46% of our survey respondents believed that their external auditors utilized a risk-based and top-down approach as required by PCAOB Auditing Standard Number 2 (AS 2). During year two, 27% believed their external auditors focused their scope of §404 work on the identification of potential material weaknesses and performed only limited work on areas that were unlikely sources of material error. During year two, only 42% stated that their external auditors conducted an integrated audit. Sixty percent of respondents stated that their external auditors performed separate tests for the purpose of the audit of internal controls and the financial statement audit.

- Of the 75% of respondents using a top-down and risk-based approach, 30% of these respondents indicated that their organization did not see a more effective and efficient external audit process. In addition, 58% of the respondents indicated the external auditors tested controls that did not relate to a risk-based approach and that could not materially impact the financial statements. This practice is tremendously ineffective, does not follow AS 2 guidance and is driving costs up without benefits.

- Although the May and November 2005 guidance from the PCAOB was discussed between management and internal and external audit, this guidance was not followed according to 31% (May) and 25% (November) of our survey participants. The reasons most often provided were that the guidance came too late in the process and/or it was not given the same weight by the external auditors because it was not a "standard" but only informal guidance. We believe that AS 2 should be amended to include the messages from the May guidance and any appropriate guidance going forward.

- Though external auditors relied on internal auditors' work to a greater extent, the degree remains relatively low. Our results indicated that 48% of our respondents committed over 51% of their total internal audit resources to §404. And while many departments dedicated over 51% of their time to §404 work, 44% responded that the extent (percentage of total cost) that the external auditors reduced their work due to reliance on internal audit's work was less than 10%. This diversion of internal audit resources for seemingly little gain in efficiencies and effectiveness cannot continue. 60% of respondents believe that their internal audit resources were diverted away from areas that were high to moderate in risk, which, if audited, would have provided greater value to the organization.

In addition, new challenges to implementation arose in year two:

- Survey results indicated that 34% of respondents believe that, to significantly reduce external audit costs, a major driver will be the alignment of PCAOB guidance and accounting firm inspections.

- 33% of the respondents whose external auditor received a PCAOB inspection report did not share the results of the report with the company. We believe that senior management, internal auditing, and the audit committee should be apprised of inspection results of the firm they employ for financial statement audits as a matter of transparency and to ensure improved future efficiencies.

In order to address a critical impediment to long-term sustainability and to achieve a cost and benefit acceptance of §404 from both corporations and investors: The IIA recommends a fundamental change be considered and AS 2 be modified accordingly. Currently three attestations are being produced to provide assurance on internal controls over financial reporting: management's attestation; the external auditor's attestation over management's attestation; and, the external auditor's own attestation over internal control.

We believe that the intent and the benefit of the Sarbanes-Oxley Act[1] are met with only two attestations – namely, management's attestation, and the external auditor's attestation over management's attestation. This approach is prevalent in other securities trading markets (e.g., Canada - Ontario Securities Commission regulation – CSA notice

---

[1] Sarbanes-Oxley Act – §404. Management Assessment of Internal Controls, (b) "Internal control evaluation and reporting – with respect to internal control assessment required by subsection (a) each registered public accounting firm that prepares or issues the audit report for the issuer shall attest to, and report on, the assessment made by the management of the issuer. An attestation made under this subsection shall be made in accordance with standards for attestation engagements issues or adopted by the Board (PCAOB). Any such attestation shall not be the subject of a separate engagement.

52 -313; and, France - Loi sur la Sécurite Financière article 117 & 120), and would provide for consistency internationally, harmonization, and fair treatment for corporation in a global economy. Also, in the United Kingdom, The Combined Code on Corporate Governance only requires boards to review the effectiveness of all internal control (not just financial control) and report publicly that they have done so. External auditors will review such reports, essentially for consistency with their knowledge gained in other work, but do not audit the disclosure in any sense equivalent to the §404 requirement. Thus, UK companies do not provide any external reporting on internal control effectiveness and do not have a requirement of attestations, either by management or external auditors. Requiring all three attestations creates a competitive disadvantage for U.S. companies, especially for those doing business abroad. If only two attestations are required, comment relating to the external auditor's attestation below would not be relevant.

The IIA recognizes that the above proposed change would require some time to consider and implement, thus, the following summarizes what we believe to be the key issues that continue to be germane for improvements to the §404 implementation process as it currently exists:

I. Additional guidance is needed for both management and audit firms
II. There remains a need for increased reliance on the work of others
III. Continued improvement in the effectiveness and efficiency of the §404 process

The above key issues should be considered a priority for expected impact on year 3. Additional suggestions that we believe will further improve the 404 process are discussed in Attachment C below. We recommend that you address those as priorities permit.

IIA's Recommendations for Improvement

I. Additional Guidance Needed for Both Management and Audit Firms

A. 75% of our survey respondents believe that additional detailed guidance for management is needed regarding the §404 control assessment process and the quarterly §302 assessment process. We believe the audit process will become more proficient when management's assessment process becomes more efficient. We encourage the U.S. Securities and Exchange Commission to consider finding ways to provide more guidance to management to promote efficiencies in management's assessment of internal controls over financial reporting. Such guidance should provide management with the knowledge and tools to properly identify risks and key controls, build the assessment processes, and provide for consistent transparent disclosures of material weaknesses and their remediation. Without such guidance, management relies on the guidance provided by PCAOB to the external auditors, which was not intended to guide management's implementation of §302 and §404.

As a means of trying to fill the void in management guidance voiced by our members, The IIA has recently issued, *Sarbanes-Oxley Section 404: A Guide for Management by Internal Control Practitioners* (Attachment B). Written for management by experienced internal auditors who have worked on internal controls hand-in-hand with their organization's external auditors, audit committees, and management, it incorporates and reflects up-to-date guidance from the SEC and PCAOB.

B. The SEC, PCAOB and/or other appropriate bodies should collaborate to ensure there is an effective resolution process for differences of opinion between registrants and their auditors. Examples include when the issue may not be quantifiable, involves judgment on something such as the sufficiency and extent of documentation that may be needed, or in situations where future events, such as loan losses, bad debts, contingent liabilities, or potential legal actions may require reserves to be established. Even if models are used to forecast potential outcomes based on past history, there is still the need to apply judgment. Professional judgment must be exercised when it comes to assessing the likelihood that exceptions found as a result of audit tests will actually result in misstatements of accounts. Feedback received in our survey indicated that this part of the §404 process was probably the most tenuous and the timely communication between management and the external auditors the most strained.

C. There is a tendency with Information Technology General Controls (ITGC), due to the incorrect and overuse of the term "pervasive," to ascribe too much significance to ITGC risks. While ITGC as a whole may affect multiple applications and multiple key automated controls, in practice, individual key controls within ITGC do not always have a "pervasive" affect but may only impact a limited number of applications or locations. Further clarification would be valuable on the use and meaning of pervasive, as well as on the related topic of aggregation. Also, by their nature, ITGC are somewhat removed from direct linkage to financial statement assertions. ITGC are critical to support computerized applications that are generally an integral part of a company's system of internal control of financial reporting (ICFR). We have observed that this linkage provides difficulties to external auditors when they are trying to define a scope for ITGC that focuses on risks that are at least reasonably likely to be the root cause of an undetected material error in the financial statements.

This appears to be caused by a sizeable amount of bottoms-up risk identification, especially when determining what ITGC issues should be in scope. The IIA, in association with a number of audit firms and companies of all sizes (including 13 of the Fortune 100) is developing a scoping methodology for ITGC that is based on risk. We anticipate this product will be available in the second half of 2006.

II. Need for Increased Reliance on Work of Others

D. The IIA promotes increased reliance on the use of the work of a competent and independent internal audit function as survey results have shown that this is an effective way to reduce external audit costs and increase efficiencies. We believe an internal audit function operating in accordance with The IIA's *International Standards for the Professional Practice of Internal Auditing* is well equipped to meet the challenges of good governance. While the PCAOB standard appears to allow the external auditor to rely on the work of internal auditors, year-two implementation (as reflected in the survey) has not shown this to be as extensive as it could be. Where internal auditing has independently done testing or performed walkthroughs that fall within the scope of the financial reporting controls, external auditors should rely on that work.

E. It should be stressed that planning by the external auditor should not only be done early, but should be shared with management to enable more effective use of and reliance on management testing. As noted by many organizations and again reflected in our survey, significant opportunities remain for improved reliance by the external auditors on management testing, including and especially testing performed by the internal auditing function.

III. Continued Improvement in the Effectiveness and Efficiency of the §404 Process

F. The importance of a top-down, risk-based approach cannot be over-emphasized. The SEC and PCAOB were correct when they indicated in May 2005 that this approach is critical to an efficient process that focuses appropriately on risks to the financial statements. However, as shown by the results of our survey, implementation of this approach has been disappointingly slow (only 46% of respondents believed external auditors used a risk-based approach).

G. The IIA encourages increased consideration of company-level controls. Guidance issued by the PCAOB subsequent to AS 2 has addressed the importance of company-level controls in executing a risk-based audit. However, the supplemental guidance has addressed this topic at a very conceptual level, while the detailed guidance of AS 2 provides numerous detailed examples of designing audit testing without reference to company-level controls.

The supplemental guidance issued after publication of AS 2 gives a strong endorsement to the need for external auditors to give early and complete consideration of company-level controls as a method to fully implement a risk-based testing approach. While this supplemental guidance has made these statements, AS 2 continues to have a number of elements that appear inconsistent with this guidance. More specifically in AS 2:

1. Paragraph 40 discusses what an external auditor should do to obtain an understanding of management's process for assessing the effectiveness of internal controls. The first element listed for the external auditor's consideration is a discussion of which controls management has decided should be tested. Company-level controls are the last item listed, transaction level controls are listed first.

2. Paragraph 52 discusses identifying company-level controls. This paragraph states: "Controls that exist at the company-level often have a pervasive impact on controls at the process, transaction, or application level. For that reason, as a practical consideration, it may be appropriate for the auditor to test and evaluate the design effectiveness of company-level controls first…" The only discussion is regarding how company-level controls impact detailed transaction level testing, and then only as a practical matter. Missing is a clear discussion of considering company-level controls as part of a risk-based audit.

3. AS 2 has numerous examples of how to determine which detailed transaction-level controls should be tested. There are no examples of how the external auditor should consider testing company-level controls as a partial substitute for detailed transaction control testing in lower risk areas. For example, none of the examples in Appendix B to AS 2 starting after paragraph B31 have any discussion or consideration of company-level controls.

4. Paragraph B1 directs the auditor to move from identifying business units that are individually important to evaluating documentation and testing controls over significant accounts. There is no discussion of company-level controls other than for individually unimportant business units.

In conclusion, The Institute believes that much has been achieved and that more can be done to enhance sound corporate governance. We think that effective and efficient corporate governance emanates from the synergy and balanced relationships between those in charge of governance -- the board and management -- and their two primary support partners, external and internal audit.

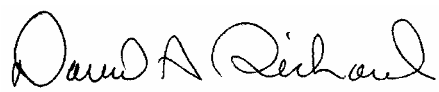
Essential to any corporate governance structure is the need to establish clear roles for all involved. Management's control responsibility covers all operations and risks and they should be provided with further guidance that help them meet the expectations of §302 and rebalance their overall control and monitoring efforts. Internal auditors should support management in carrying out its responsibilities but not take on management's responsibilities for documenting controls or implementing systems of internal controls. The investors and shareholders should be equally concerned with all risks and related controls that may impact the sustainable performance of the businesses in which they invest, and not just those risks and controls that relates to financial reporting. The SEC and PCAOB should support this approach.

Professional internal auditors, performing their duties in compliance with the *International Standards for the Professional Practice of Internal Auditing,* are traditionally the ones who provide an objective assessment of internal control over core risk areas of the organization on an on-going basis. It is essential to recognize that internal auditing has been diverted (to varying degrees) to support management's §404 effort instead of being complemented (i.e., additional resources provided) to continue its essential tasks
Ms. Nancy M Morris

as well as support management in the implementation and on-going monitoring of the SOX §404 effort. It would be appropriate for both the SEC and PCAOB to reinforce this key message.

Representatives from The IIA will be attending the SEC and PCAOB roundtable meeting in Washington on May 10 and we welcome the opportunity to discuss any and all of these issues with you.

Best regards,



David A. Richards, CIA

Attachments

A – Year 2 Sox Implementation Survey Results

B – *Sarbanes-Oxley Section 404: A Guide for Management by Internal Control Practitioners*

C – Additional Issues of Interest to be Considered

About The Institute of Internal Auditors

The IIA is the global voice, acknowledged leader, principal educator and recognized authority of the internal audit profession and maintains the *International Standards for the Professional Practice of Internal Auditing (Standards)*. These principles-based standards are recognized throughout the world and are available in 25 languages. The IIA represents more than 120,000 members across the globe, and has 247 affiliates in 92 countries that serve members at the local level.

The IIA also administers the Certified Internal Auditor (CIA) examination, given in 16 languages. The four-part test assesses the knowledge, skills, and abilities needed to be an effective internal auditor. Worldwide there are more than 57,000 CIAs.

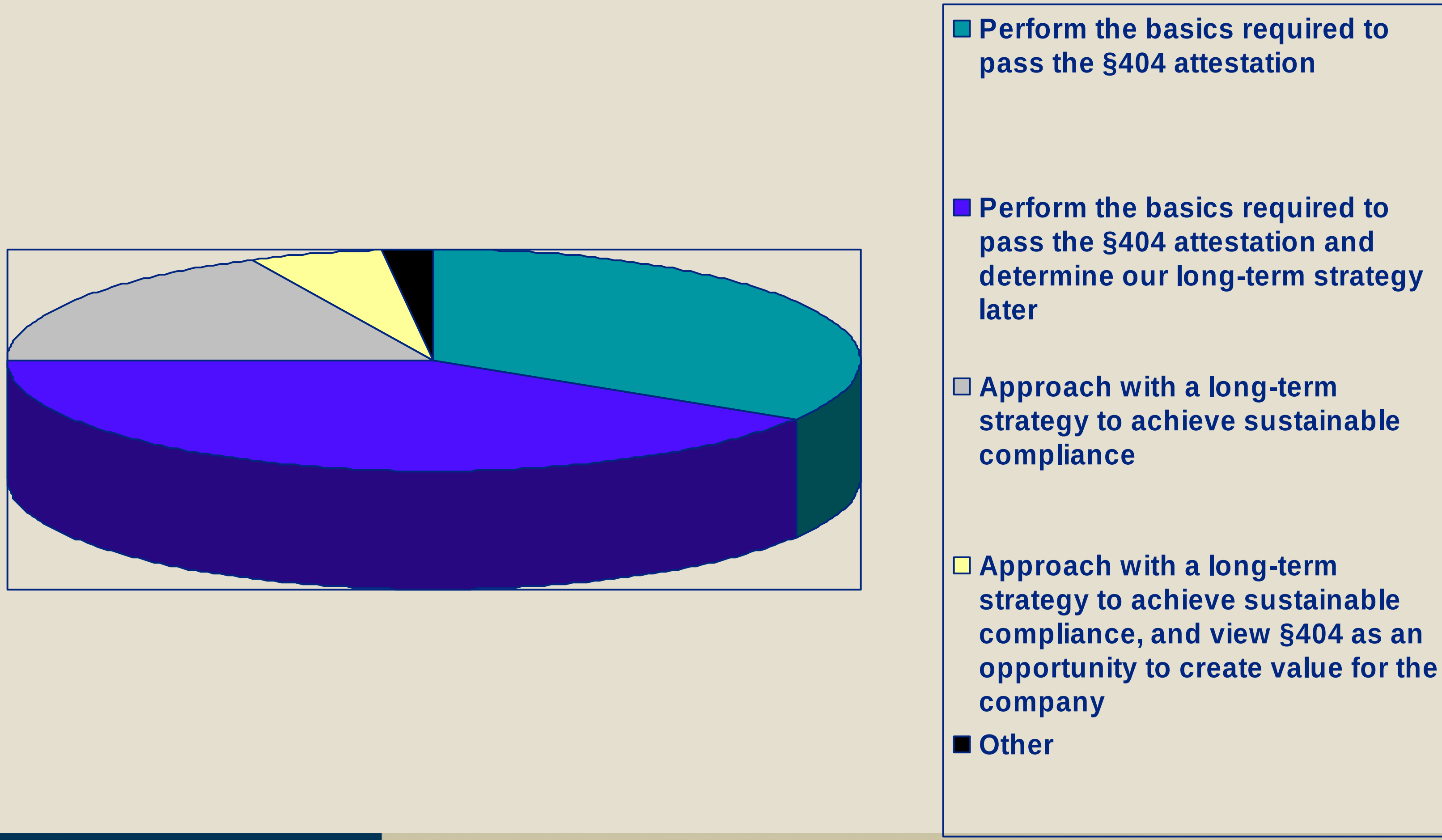
The Standards and Code of Ethics are part of The IIA's Professional Practices Framework (PPF) that also includes Practice Advisories (help interpret the *Standards*), and other guidance (e.g., position papers, research studies, books, seminars, conferences, and services related to the practice of internal auditing). The PPF provides practitioners throughout the world with a full range of guidance, products and services for high-quality internal auditing services.

Year 2 SOX Implementation

Live Date: 3/31/2006
Close Date: 4/12/2006
Invitations: 1,365
Responses: 131 (9.8%)

Presentation Generated: 4/19/2006

Looking at year 1, which of the following best reflects your organization s Sarbanes-Oxley §404 philosophy and objective?



Looking at year 1, which of the following best reflects your organization s Sarbanes-Oxley §404 philosophy and objective?

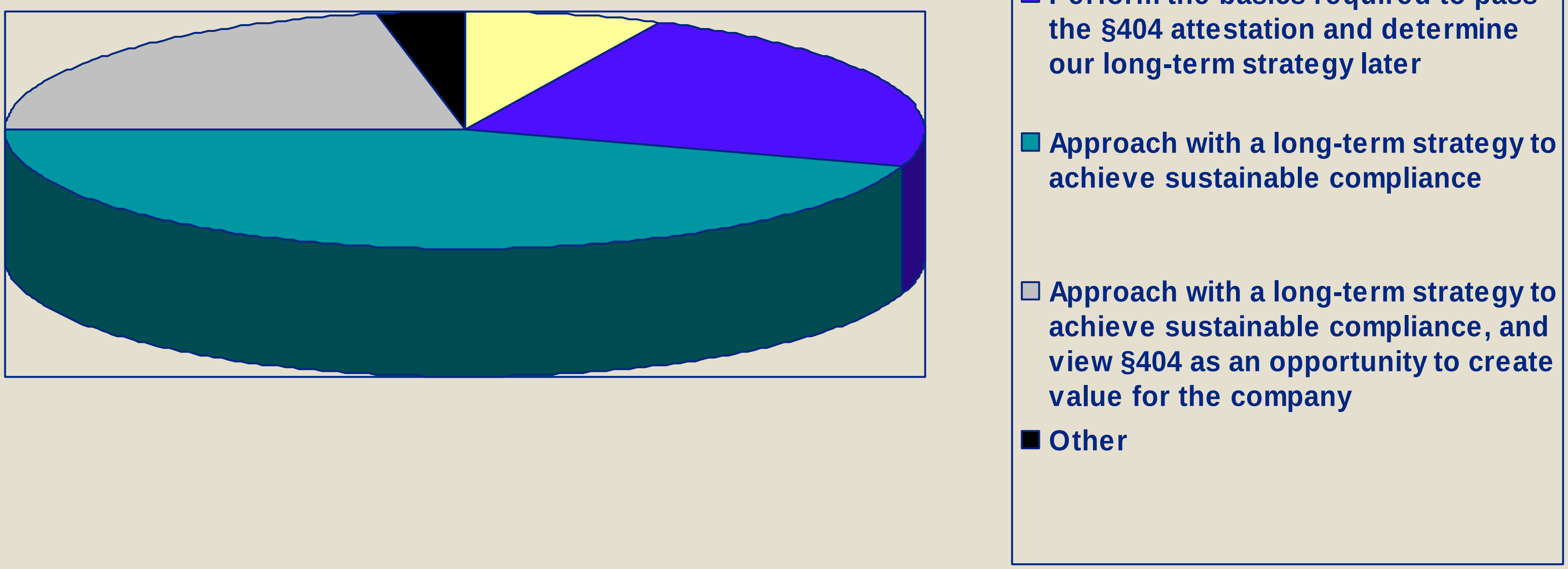
Choice	Count	Percentage of Sample Answering	Percentage of Total Sample
Perform the basics required to pass the §404 attestation	43	33.6%	32.8%
Perform the basics required to pass the §404 attestation and determine our long-term strategy later	52	40.6%	39.7%
Approach with a long-term strategy to achieve sustainable compliance	23	18.0%	17.6%
Approach with a long-term strategy to achieve sustainable compliance, and view §404 as an opportunity to create value for the company	7	5.5%	5.3%
Other (see below)	3	2.3%	2.3%

Looking at year 1, which other statements best reflects your organization s Sarbanes-Oxley §404 philosophy and objective?

Performed far beyond the basics to pass

Perform with over-conservatism the thought requirements to pass S.404 (rules came in late)

Looking at year 2, which of the following best reflects your organization s Sarbanes-Oxley §404 philosophy and objective?



Looking at year 2, which of the following best reflects your organization s Sarbanes-Oxley §404 philosophy and objective?

Choice	Count	Percentage of Sample Answering	Percentage of Total Sample
Perform the basics required to pass the §404 attestation	9	7.1%	6.9%
Perform the basics required to pass the §404 attestation and determine our long-term strategy later	29	22.8%	22.1%
Approach with a long-term strategy to achieve sustainable compliance	57	44.9%	43.5%
Approach with a long-term strategy to achieve sustainable compliance, and view §404 as an opportunity to create value for the company	28	22.0%	21.4%
Other (see below)	4	3.1%	3.1%

Looking at year 2, which other statements best reflects your organization s Sarbanes-Oxley §404 philosophy and objective?

Defining long term strategy is in process but is not yet well defined.

Significantly rescope the year 1 compliance based on 5/16/05 guidance considering long term strategy - refining LT strategy in Year 3

Streamline and sustain program

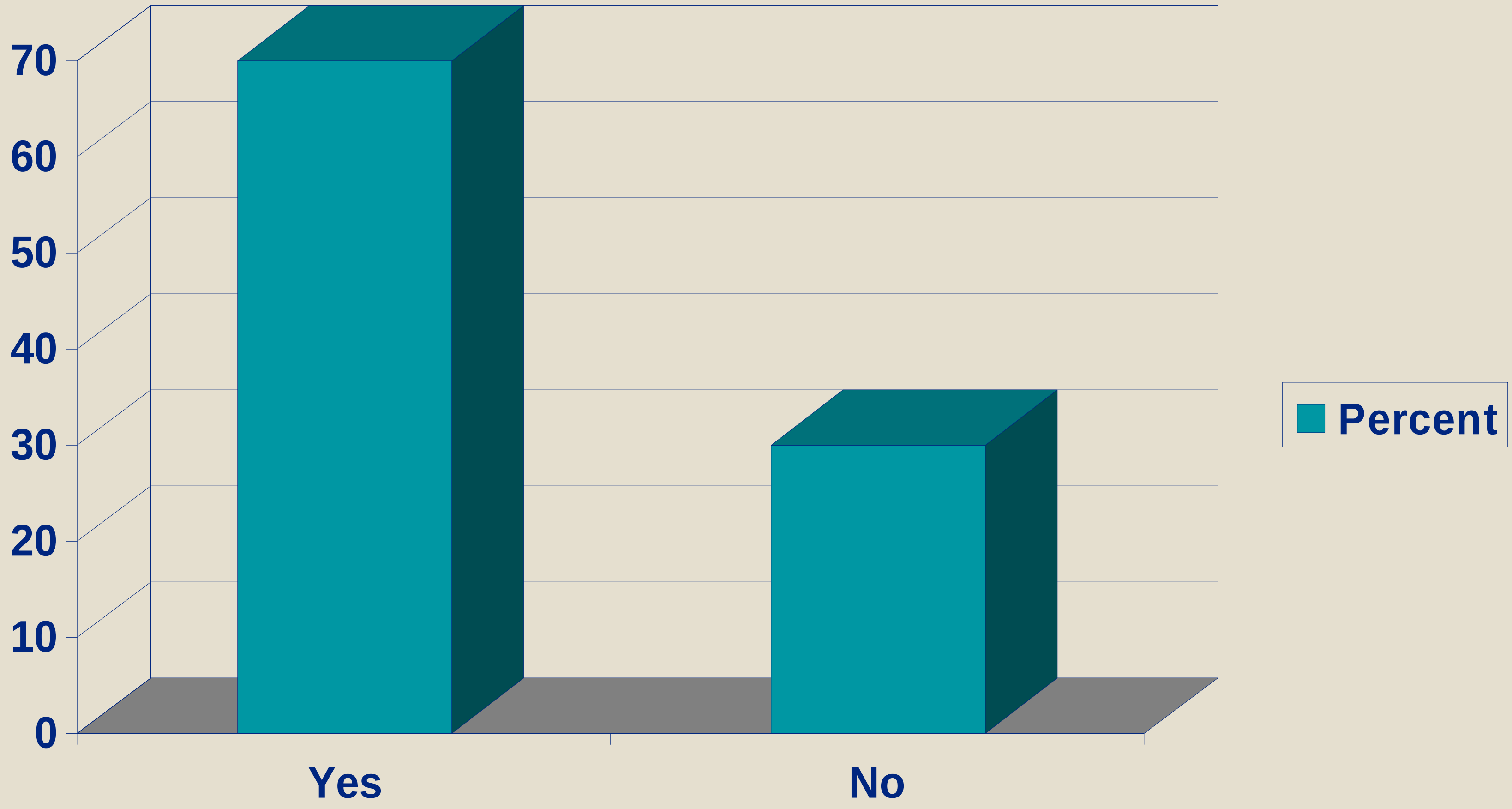
How strongly do you agree or disagree with the following statements regarding the implementation of a top-down and risk-based approach to SOX looking at year 1?

Topic	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Our organization utilizes a top-down approach to define the scope of work for §404	13	33	22	38	18
Our organization utilizes a risk-based approach to define the scope of work for §404	7	27	28	47	14
Our external auditors utilize a top-down approach to define the scope of work for §404	27	41	21	31	4
Our external auditors utilize a risk-based approach to define the scope of work for §404	25	38	25	34	3
Our external auditors have focused their scope of work for §404 on the identification of potential material weaknesses and performed only limited work on areas that are unlikely sources of material error	42	48	15	15	4
Our external auditors conducted an integrated audit	46	40	12	22	3

How strongly do you agree or disagree with the following statements regarding the implementation of a top-down and risk-based approach to SOX looking at year 2?

Topic	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Our organization utilizes a top-down approach to define the scope of work for §404	2	10	15	60	38
Our organization utilizes a risk-based approach to define the scope of work for §404	3	5	11	63	42
Our external auditors utilize a top-down approach to define the scope of work for §404	9	34	21	48	11
Our external auditors utilize a risk-based approach to define the scope of work for §404	10	33	19	52	8
Our external auditors have focused their scope of work for §404 on the identification of potential material weaknesses and performed only limited work on areas that are unlikely sources of material error	24	49	18	26	5
Our external auditors conducted an integrated audit	14	26	26	41	14

If your organization utilized a top-down and/or risk-based approach, did it result in a more effective and efficient external audit process?



If your organization utilized a top-down and/or risk-based approach, did it result in a more effective and efficient external audit process?

Choice	Count	Percentage of Sample Answering	Percentage of Sample Asked	Percentage of Total Sample
Yes	79	69.9%	60.3%	60.3%
No (explanation below)	34	30.1%	26.0%	26.0%

If your organization utilized a top-down and/or risk-based approach, why did it not result in a more effective and efficient external audit process?

Had to change our approach to meet requirements/standards of external auditors

External Auditors still testing very low level risk areas in a very detailed manner

External Auditors substantially ignored our approach and went with their own.

The external audit process was strenuous, overly repetitive and ineffective. There was too much duplication of efforts and testing for controls that were not key or that would not indicate a material issue. WE wasted too much money

Wasn't effectively applied by the organization.

Externals were so risk averse, they expanded scope of controls and testing to get to more than reasonable assurance that controls were working

Inefficiency of External Auditors and Paranoid of PCAOB so over audited - CYA approach

Had to add additional work to satisfy external auditors.

The external auditors continue to fear liability and believe that they must do more work than necessary. the improved from year one, however they need to embrace a risk based approach and better coordinating their effort w/us, and being more transparent.

External auditor ignored the top/down risk analysis

If your organization utilized a top-down and/or risk-based approach, why did it not result in a more effective and efficient external audit process? (Continued)

404 testing outsourced & coordination with external audit needs improvement. Focus of yr 3

Inflexibility of External Auditor

Cannot tell. I do not think our approach would changed the auditors approach to be more efficient and effective.

External Auditors continue to use a "checklist" approach to controls at the process level. I speculate that their is some fear of the PCAOB reviews that results in a very conservative approach.

duplication

Overall, answer is yes - but still a lot of continued progress in this direction

We utilized top-down but it did not materially result in a more effective and efficient external audit

New external auditors in 2004

We had identified too many key controls

Externals followed their own path

The external auditors appeared to be focused only on those areas that they thought were risky despite the results of management's "top-down" analysis.

If your organization utilized a top-down and/or risk-based approach, why did it not result in a more effective and efficient external audit process? (Continued)

Efficiencies can not be realized due to limitations place on the company by its external auditors.

the external auditors didn't seem interested in our approach. We felt they took a "witch hunt" approach designed to fill a quota of deficiency whose number was communicated at least 6 months prior to their beginning SOX work.

The external auditors still went through their routine, same as years past.

Our external auditors appeared to be fixated on the areas of concern despite the results of management's "top-down" assessment.

External auditors have somewhat different objectives vs. our objectives

The external auditors (monopolists) have no incentive to be efficient in their work product. The longer the audit takes (cost plus), the more money they make.

Believed they still looked at a lot of areas that were not high risk just because it was year one and new process

Externals did not rely on internal work

If your organization did not utilize a top-down and/or risk-based approach, what approach did you use?

The organization mirrored the approach by the external auditors of beginning at the transaction level and worked up the significant account. In addition, Entity / Company level controls were tested last and up to the point we filed our annual report on Form 10-K.

Answering questions from a consulting perspective as to generally what I have seen in the organizations we have assisted in 404 compliance, so some questions are N/A

Attempted top-down approach, but external auditors required additional work.

Documented all key controls and tested regardless of risk.

Defining significant process level controls and testing those considered to be most important or testing those that do not have any other mitigating or compensating control.

ERM process implemented. Performed a risk assessment based on standard probability and impact considerations for financial statement elements.

In year 2, we were still very much focused on individual key controls as the external auditor was reluctant to relinquish this type of testing.

Used a top down / risk based approach, but also still review the control environment from a process standpoint which makes it harder to reduce control points.

Still selecting transactional processes

If your organization did not utilize a top-down and/or risk-based approach, what approach did you use? (Continued)

Financial statement balances

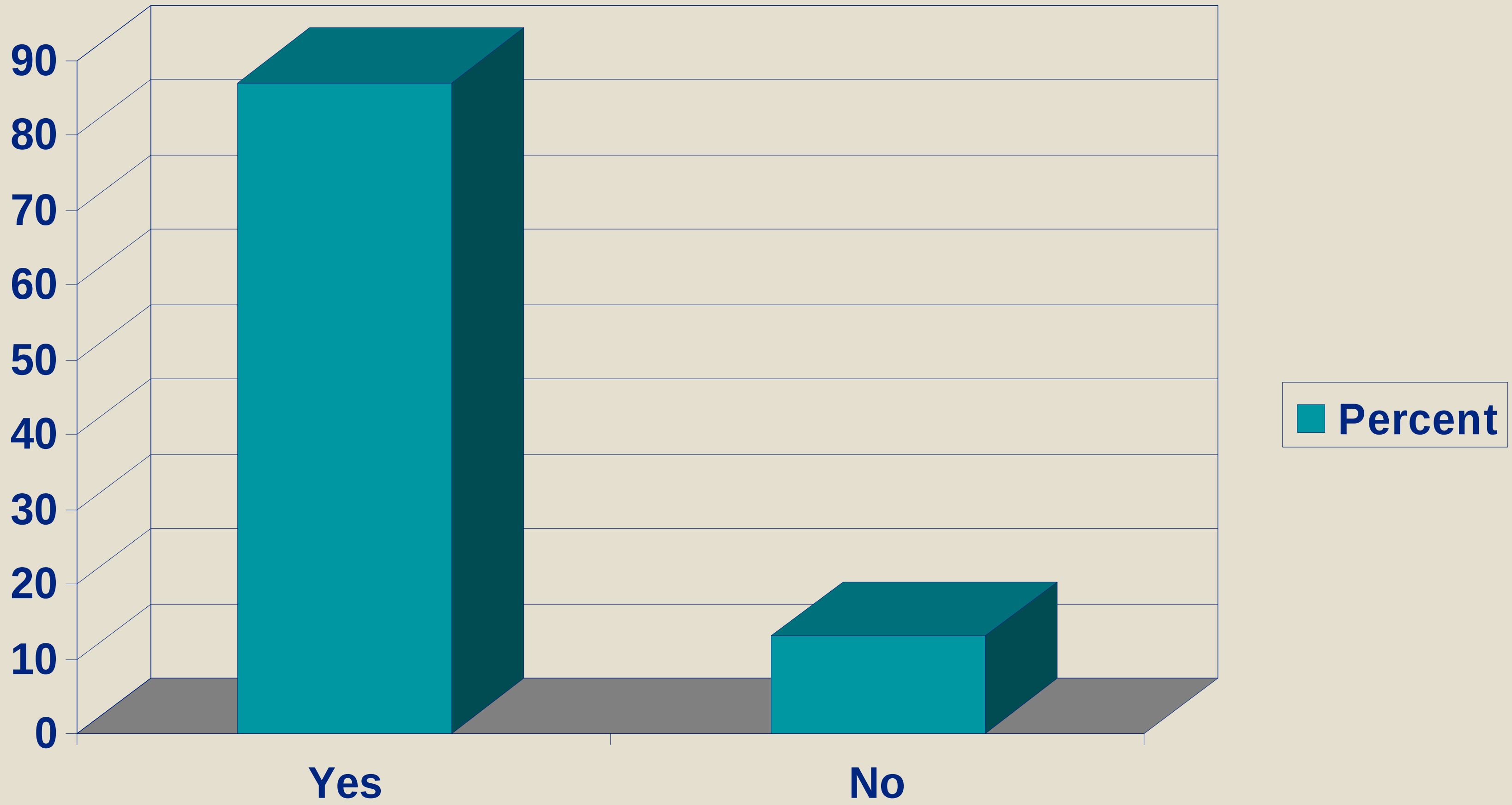
Account materiality

Risk based utilizing a COSO benchmarking exercise performed several years ago as incorporated into the Internal Audit Department rick evaluation and planning process

How strongly do you agree or disagree with the following statements:

Topic	Strongly disagree	Disagree	Neutral	Agree	Strongly agree	No basis for opinion
Our internal audit resources have been diverted away from areas that are high to moderate in risk, that if audited would provide greater value to the organization	5	25	11	44	35	6
Our organization s Sarbanes-Oxley §404 efforts have increased the reliability of internal controls over financial reporting (ICFR)	5	5	17	60	39	0
Additional detailed guidance from the SEC/PCAOB to management is needed regarding the annual §404 control assessment process and quarterly §302 assessment process	1	9	17	41	57	1
Additional guidance from the SEC/PCAOB to management is needed on operational, compliance, and strategic risks, so that all aspects of strong governance are considered and addressed by publicly traded companies	11	23	16	34	40	2
The audit committee provides significant oversight for the work of the external auditors	3	17	33	43	28	1

Have you discussed the use of the May 16th 2005 SEC/PCAOB guidance with your external auditors to reassess §404 planning and design for year 2?



Progress Through Sharing

Have you discussed the use of the May 16th 2005 SEC/PCAOB guidance with your external auditors to reassess §404 planning and design for year 2?

Choice	Count	Percentage of Sample Answering	Percentage of Sample Asked	Percentage of Total Sample
Yes	109	87.2%	83.2%	83.2%
No (explanation below)	16	12.8%	12.2%	12.2%

Why have you <u>not</u> discussed the use of the May 16th 2005 SEC/PCAOB guidance with your external auditors to reassess §404 planning and design for year 2?

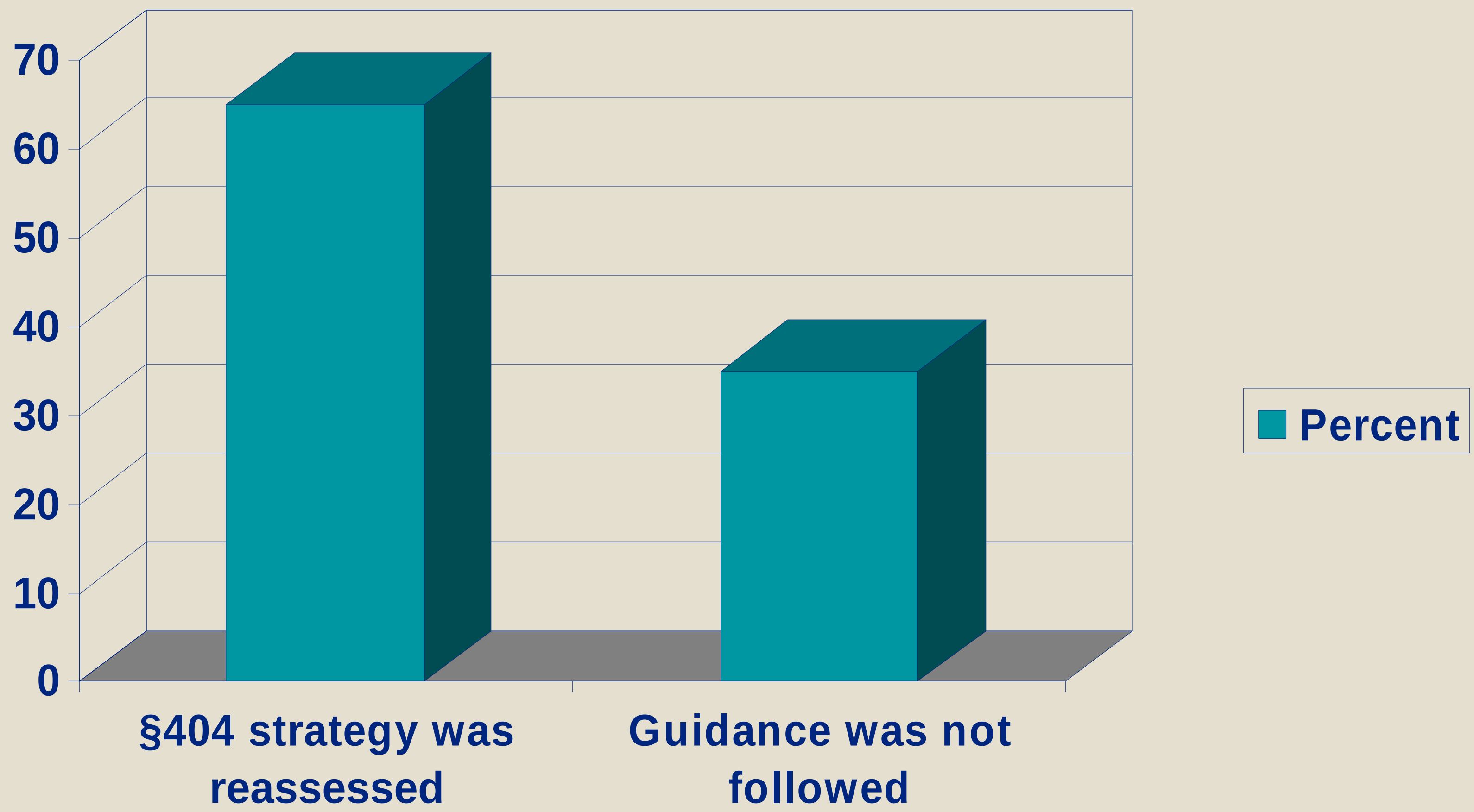
- We modified our approach without discussing with external auditors.
- Our auditors indicated that while the PCAOB has written publicly that top down risk based was the preferred method, they are getting written up for not doing enough transaction level testing by the PCAOB.
- still working on ANNUAL CONTROLS
- We're following the guidance.
- They were always digesting and never implementing or coordinating with us
- Guidance confirmed our own views. External auditor will need to reconsider their approach, especially re substance over form.
- Will implement in yr 3
- Again, partially ... but it is hard to modify approach mid-year and we still need continued progress
- They haven't asked
- Our external auditors advised that the firm's guidelines are more stringent than that of the SEC/PCAOB and used this to justify higher fees.
- Our year end is 8/31 and we actually implemented at top down, risk based approach before the guidance was issued.

Why have you not discussed the use of the May 16th 2005 SEC/PCAOB guidance with your external auditors to reassess §404 planning and design for year 2? (Continued)

They appear firm on their approach and required independence

This is too late in the year. We're already well underway!

If you have discussed the use of the May 16th 2005 SEC/PCAOB guidance with your external auditors, what was the result of this discussion?



If you have discussed the use of the May 16th 2005 SEC/PCAOB guidance with your external auditors, what was the result of this discussion?

Choice	Count	Percentage of Sample Answering	Percentage of Sample Asked	Percentage of Total Sample
§404 strategy was reassessed	75	64.7%	57.3%	57.3%
Guidance was not followed (explanation below)	41	35.3%	31.3%	31.3%

If you have discussed the use of the May 16th 2005 SEC/PCAOB guidance with your external auditors, please explain why the guidance was not followed?

- Guidance was too late for external auditors to evaluate and change their guidelines and approach for year 2
- Auditors' work programs were not timely updated, they were still required to do much more than what the guidance suggested
- we said we would, but in reality it was not achieved
- The external auditors do not have clear guidance from the PCAOB and until AS2 is amended to reflect the top down risk based approach that is the strict standard they are held to.
- External "Big 4" audit firm apparently disagrees that the May 16 guidance is authoritative and imposed the same strict, rule-based testing requirement on management. Year 2 was a replay of year 1.
- we said we would, but in reality it was not achieved
- Little appetite on the firm's part to change their approach
- Auditors felt the May 16th guidance provided little insight into revising the process. They felt the guidance was contradictory to recommendations the PCAOB was giving as a result of the public firms reviews.
- external auditors stuck with their Year 1 plan for Year 2

If you have discussed the use of the May 16th 2005 SEC/PCAOB guidance with your external auditors, please explain why the guidance was not followed? (Continued)

- Auditors basically stated that the public statements of the PCAOB were not consistent with their reveiw and evaluation of the audit workpapers and the auditors approach to their engagements.
- some changes were made but not all; reasonable assurance still not the threshold
- Not adequately discussed and certainly not incorporated
- Externals felt PCAOB said one thing but held them to a separate standard
- External auditors believe that the PCAOB examiners practices do not align with what the PCAOB said in their guidance.
- PCAOB did not change any rules or laws - AS2 was not changed.
- Planning was essentially complete when the guidance came out. It helped a little around the margin.
- PEA has no reason to comply - billings rule their interpretations.
- Because it is guidance, not the law
- The guidance came to late for Big 4 to digest and revise 2006 guidance. We had a specific example where our auditor was not aware of the content of an aspect of May 16th guidance.
- Partially re-assessed - more to come

If you have discussed the use of the May 16th 2005 SEC/PCAOB guidance with your external auditors, please explain why the guidance was not followed? (Continued)

Company doesn't believe scope was significantly reduced. Auditor does.

I don't know why

A top down approach or integrated audit was not utilized. External auditors continue to focus on signatory evidence of management reviews as a primary control instead of evaluating whether process controls ensure adequate assurance of financial reporting

The guidance appeared to be contradictory with the comments received from the PCAOB during their file reviews of the external auditors. Hence, without specific audit guidance issued from the PCAOB, changes would be more incremental than the May guidance.

Year 2 was already underway so used in planning for year 3 in 06

External Auditors were risk avoidant

Similar approach to year one was still used.

Our external auditors advised that the firm's guidelines are more stringent than that of the SEC/PCAOB and used this to justify higher fees.

They are very skeptical of the PCAOB based on the results of their reviews.

Guidance was too vague

If you have discussed the use of the May 16th 2005 SEC/PCAOB guidance with your external auditors, please explain why the guidance was not followed? (Continued)

extensive detailed testing, not documented= doesn't count, ITGC far fetched

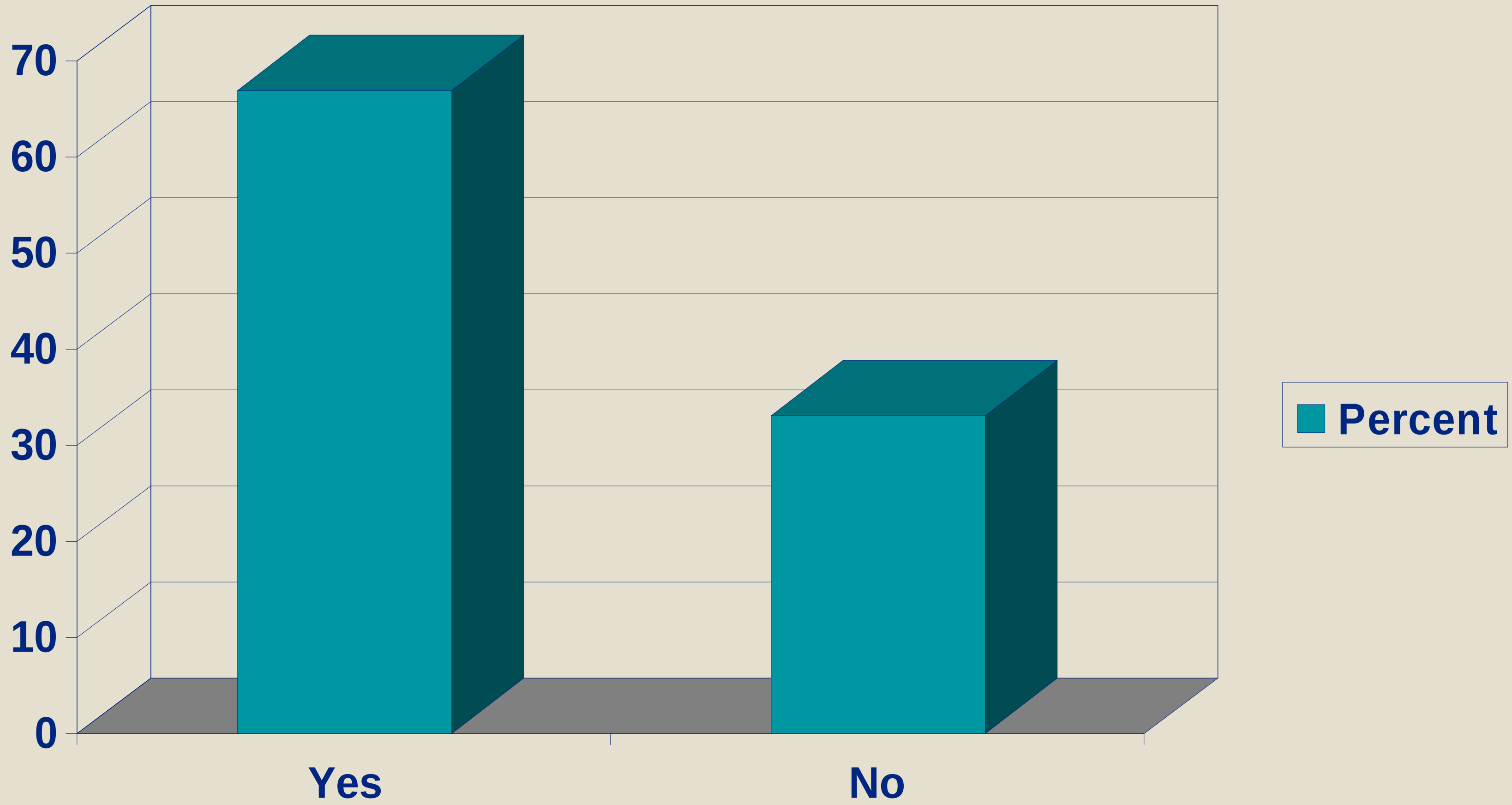
DT used an objective (database) approach not a risk based approach.

External Auditors internal guidance not updated.

Followed by external auditors until last 4 weeks prior to scheduled 10-K filing

they say they followed it but they didn't - there was no judgment of real risk but instead a cookie-cutter approach using their standard benchmarks

Have you discussed the use of the November 2005 PCAOB guidance surrounding results from PCAOB inspections with your external auditors?



Have you discussed the use of the November 2005 PCAOB guidance surrounding results from PCAOB inspections with your external auditors?

Choice	Count	Percentage of Sample Answering	Percentage of Sample Asked	Percentage of Total Sample
Yes	84	67.2%	64.1%	64.1%
No (explanation below)	41	32.8%	31.3%	31.3%

Please explain why you have <u>not</u> discussed the use of the November 2005 PCAOB guidance surrounding results from PCAOB inspections with your external auditors?

Unaware of the importance of it.

Have not had time

Not considered important at the time

Topic has not yet bee considered

New internal audit organization under creation

this is our first year

Nov release was too late for a meaningfull to impact year 2. will be discussing next week with ext auditors as it applies to year 3

I will now.

Not discussed, don't know why

upcoming meeting scheduled

Too late to impact effort

Didn't know about it.

minimal impact on our SOX Plan

Provides little additional guidance.

Please explain why you have <u>not</u> discussed the use of the November 2005 PCAOB guidance surrounding results from PCAOB inspections with your external auditors? (Continued)

Timing

Changed auditors; therefore new process implemented

Our team has been focused on completing the 2005 year end work so that the external auditor could complete their audit work. Otherwise, I am not sure why it has not been discussed.

Not Sure

opportunity has not presented itself

Late in the process, too busy completing testing. External auditor did not bring this up with Company.

Internal Audit only performs management testing.

November 2005 guidance applies to external auditors and generally does not impact companies.

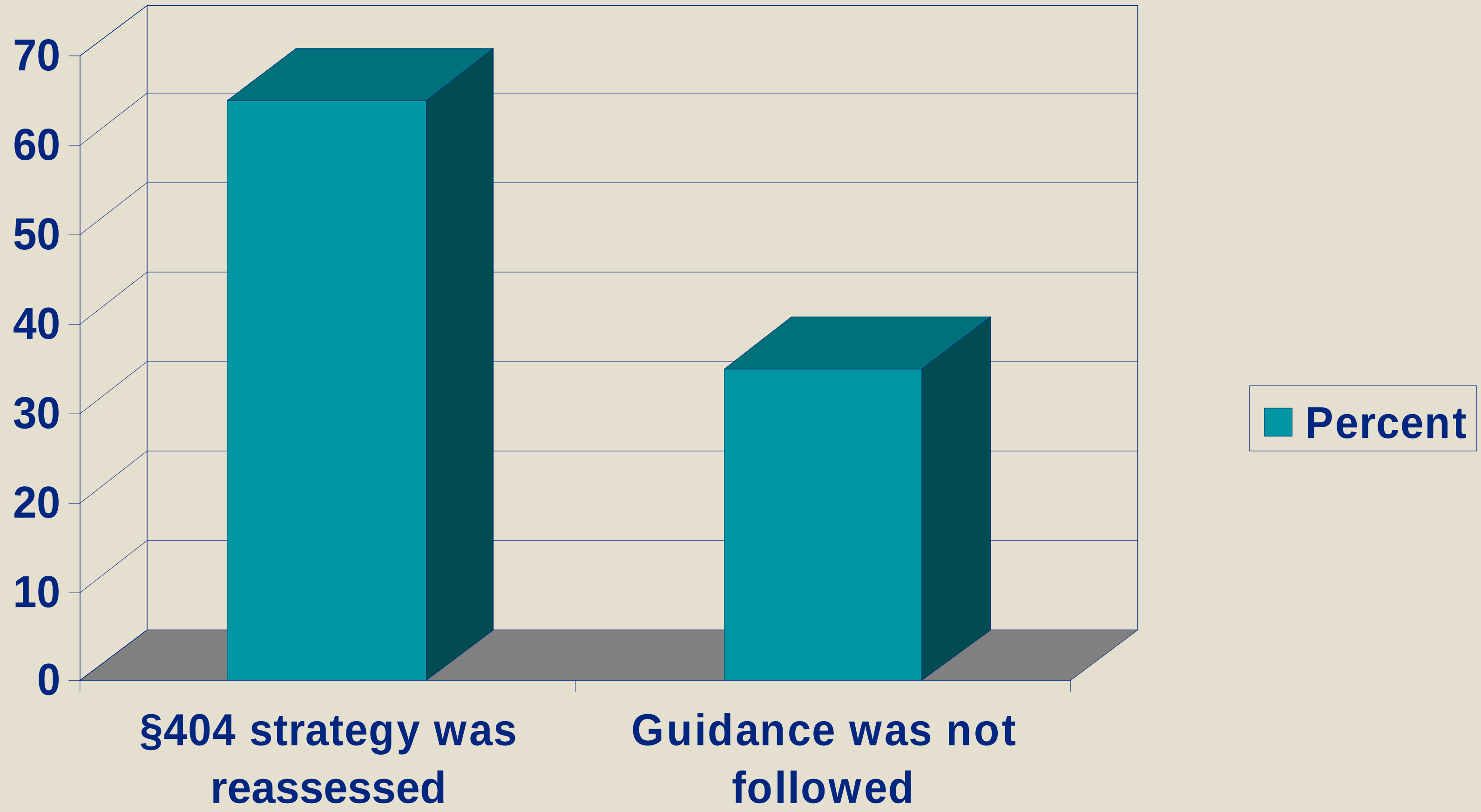
Our external reviews have been overly compliant - rather than undercompliant. Without greater definition of expectations, we are doing the maximum to ensure compliance.

Not available timely

May have been discussed with management but IA did not discuss with them.

We still have to complete our work and don't have time to strongly police the externals (which is a huge consequence of SOX compliance)!

If you have discussed the use of the November 2005 PCAOB guidance with your external auditors, what was the result of this discussion?



If you have discussed the use of the November 2005 PCAOB guidance with your external auditors, what was the result of this discussion?

Choice	Count	Percentage of Sample Answering	Percentage of Sample Asked	Percentage of Total Sample
§404 strategy was reassessed	61	64.9%	46.6%	46.6%
Guidance was not followed (explanation below)	33	35.1%	25.2%	25.2%

If you have discussed the use of the November 2005 PCAOB guidance with your external auditors, why was the guidance not followed?

- Auditors' work programs were not timely updated, they were still required to do much more than what the guidance suggested
- Until AS2 is amended, they are not changing their approach.
- Too late to make a difference in 2005, will discuss for 2006.
- Firm has not developed approach so local team followed previous approach
- Their work didn't seem to veer from the previous year, except they were distinctly paranoid in Year 2.
- Timeliness of the findings and the difference is circumstances from audit to audit made it difficult to make meaningful adjustments to scope or audit approach
- too busy...never got to it
- issued too late to change much for 2005; will be assessed for 2006
- CYA audit approach because they are paranoid about PCAOB
- External auditors over reacted to PCAOB inspections and applied findings in a very narrow, overly conservative approach.
- Externals dictate too conservatively

If you have discussed the use of the November 2005 PCAOB guidance with your external auditors, why was the guidance not followed? (Continued)

Same as above.

Big -four firm has not communicated guidance to local practice offices or has not changes the firm approach.

We were very close already

Already following key points internally.

PCAOB findings on PEA work not consistent with printed guidance and AS-2.

external auditors said that the PCAOB reports on inspections of their firm was telling them a different story

I believe the PCAOB results were not helpful and reinforced to the auditors that more and greater testing was needed

See comments above. Similar for November. The changes in the audit approach by the external auditors was less influenced by the guidance than their experiences with file reviews and direct communication with the PCAOB.

Same as above.

Guidance was too vague

If you have discussed the use of the November 2005 PCAOB guidance with your external auditors, why was the guidance not followed? (Continued)

fearful of a bad review, document and test everything

No change noted in their approach

deferred until yr 3

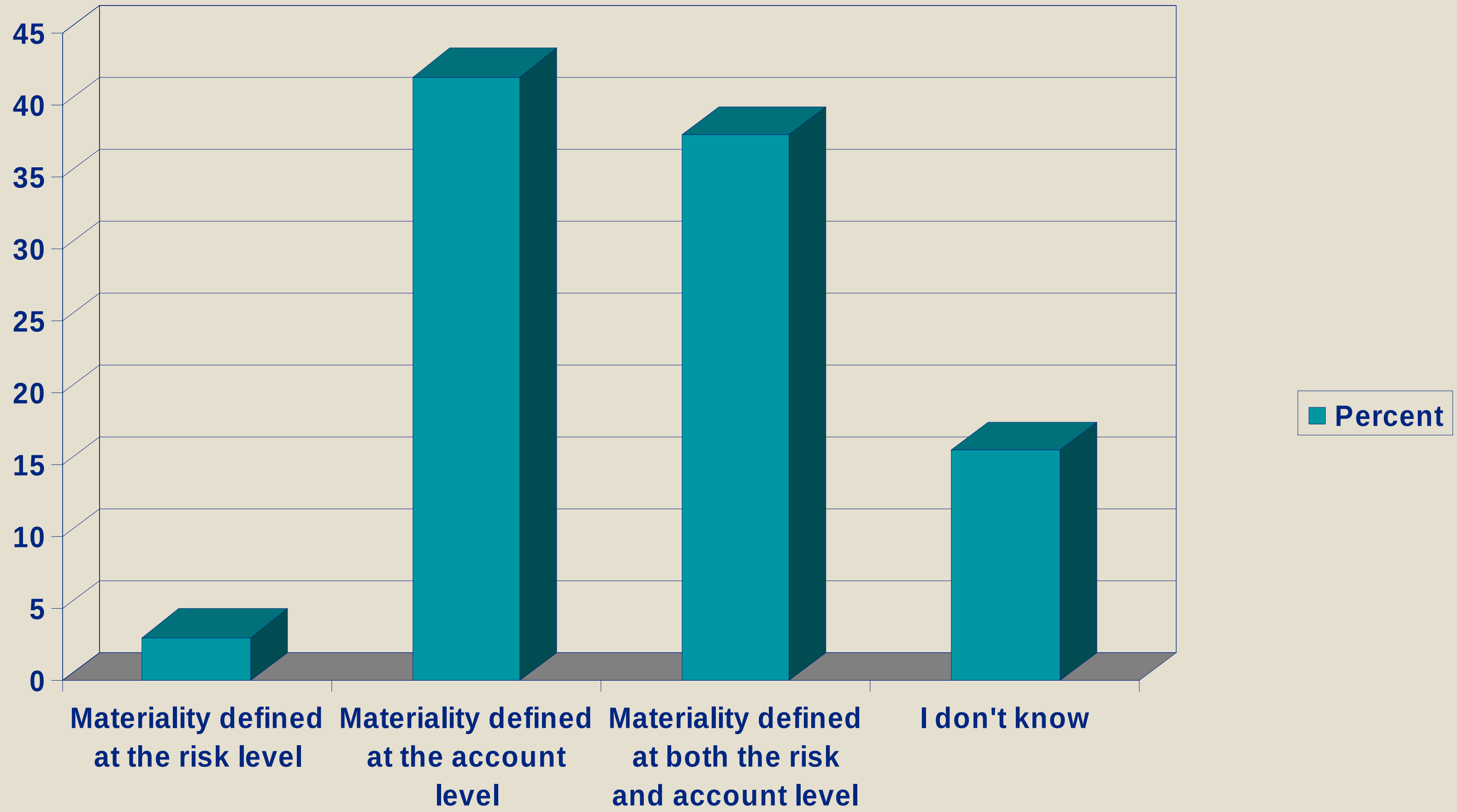
November 2005 guidance applies to external auditors and generally does not impact companies.

The audit firms use their standard benchmarks and appear afraid to exercise any real judgment. They're 100% focused on surviving a PCAOB audit, not on identifying real risks to the financials.

Did not discuss

not much information

The external auditors utilized what methods to assess a level of materiality to define the scope of work for §404:



The external auditors utilized what methods to assess a level of materiality to define the scope of work for §404:

Choice	Count	Percentage of Sample Answering	Percentage of Sample Asked	Percentage of Total Sample
Materiality defined at the risk level	4	3.2%	3.1%	3.1%
Materiality defined at the account level	53	42.4%	40.5%	40.5%
Materiality defined at both the risk and account level	48	38.4%	36.6%	36.6%
I don t know	20	16.0%	15.3%	15.3%

Please evaluate the following statements with regards to materiality for year 1:

Topic	Never	Sometimes	Usually	Always	No Answer
Management/internal audit has an understanding of the level of materiality used by the external auditors to define the scope of work for §404	8	54	44	20	5
Management/internal audit agrees with the level of materiality used by the external auditors to define the scope of work for §404	9	62	42	8	10

Please evaluate the following statements with regards to materiality for year 2:

Topic	Never	Sometimes	Usually	Always	No Answer
Management/internal audit has an understanding of the level of materiality used by the external auditors to define the scope of work for §404	5	21	55	34	16
Management/internal audit agrees with the level of materiality used by the external auditors to define the scope of work for §404	5	52	41	15	18

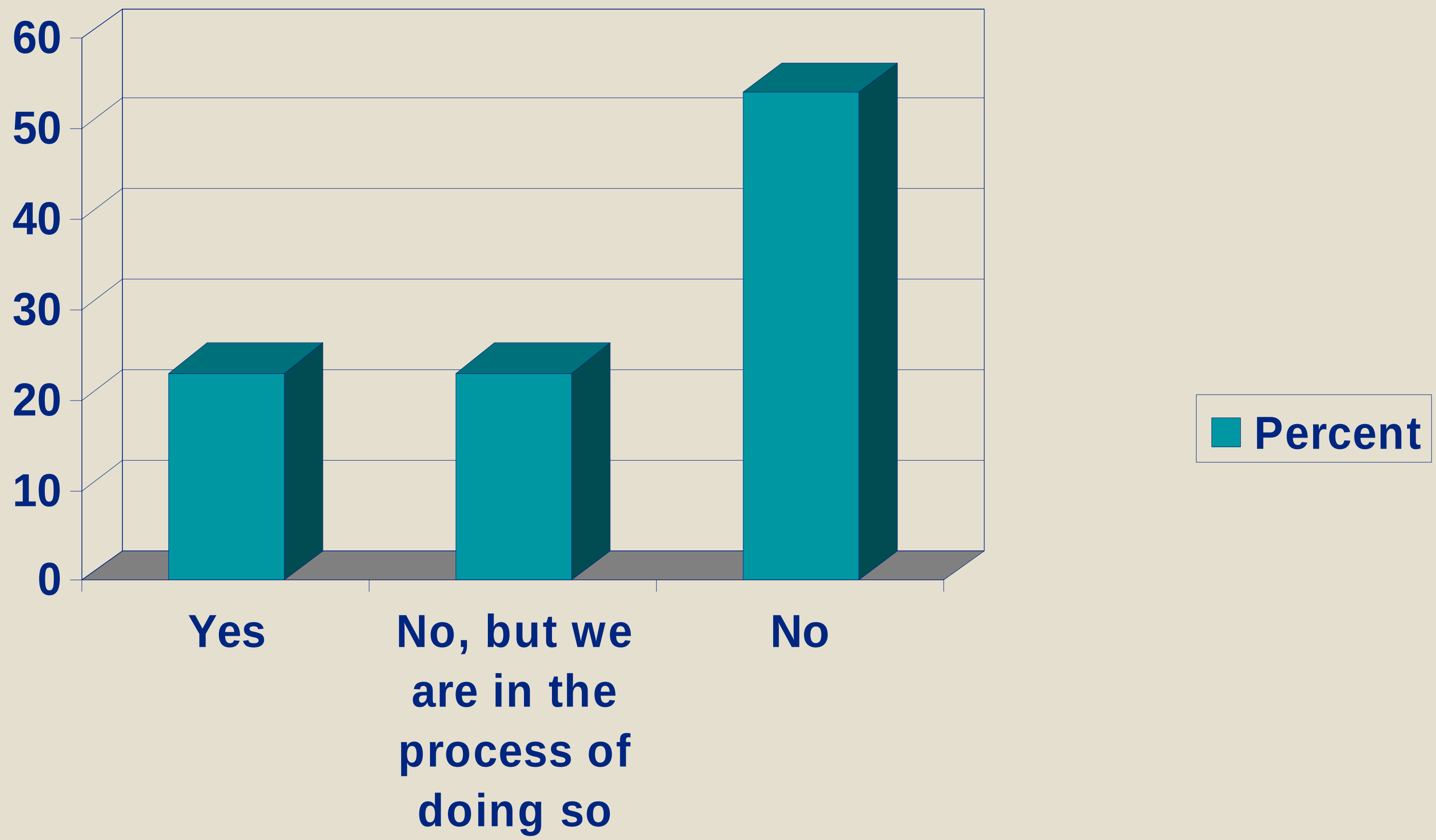
Please evaluate the following statements covering internal and external auditing relationships for year one:

Topic	Never	Sometimes	Usually	Always	No Answer
Management and internal auditors have an understanding of the nature and extent of planned external audit procedures	12	66	41	8	4
Internal and external auditors work together in coordinating audit activities	24	49	37	16	5
Internal and external auditors work together to eliminate duplicative work	38	56	20	12	5
Internal and external auditors coordinate to detect fraudulent financial reporting	44	48	26	8	5
Internal and external auditors coordinate to ensure some degree of unpredictability in their audit process related to material fraud misstatement (i.e., SAS 99)	46	42	27	10	6

Please evaluate the following statements covering internal and external auditing relationships for year two:

Topic	Never	Sometimes	Usually	Always	No Answer
Management and internal auditors have an understanding of the nature and extent of planned external audit procedures	2	40	68	15	6
Internal and external auditors work together in coordinating audit activities	5	41	53	26	6
Internal and external auditors work together to eliminate duplicative work	15	49	43	17	7
Internal and external auditors coordinate to detect fraudulent financial reporting	30	52	27	14	8
Internal and external auditors coordinate to ensure some degree of unpredictability in their audit process related to material fraud misstatement (i.e., SAS 99)	34	43	33	15	6

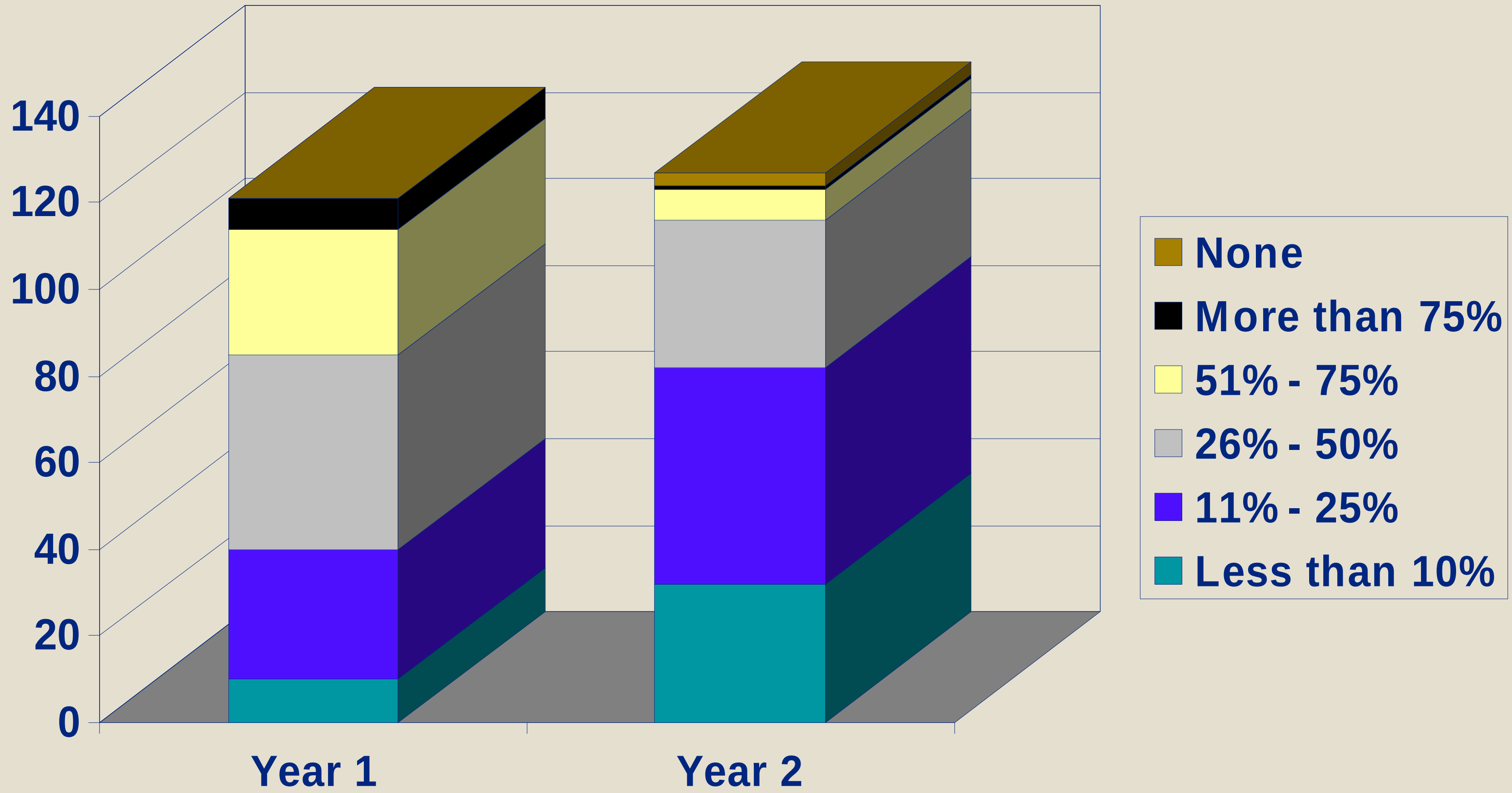
Has management implemented a forensic activity to establish a fraud prevention and detection program?



Has management implemented a forensic activity to establish a fraud prevention and detection program?

Choice	Count	Percentage of Sample Answering	Percentage of Sample Asked	Percentage of Total Sample
Yes	29	23.2%	22.1%	22.1%
No, but we are in the process of doing so.	29	23.2%	22.1%	22.1%
No	67	53.6%	51.1%	51.1%

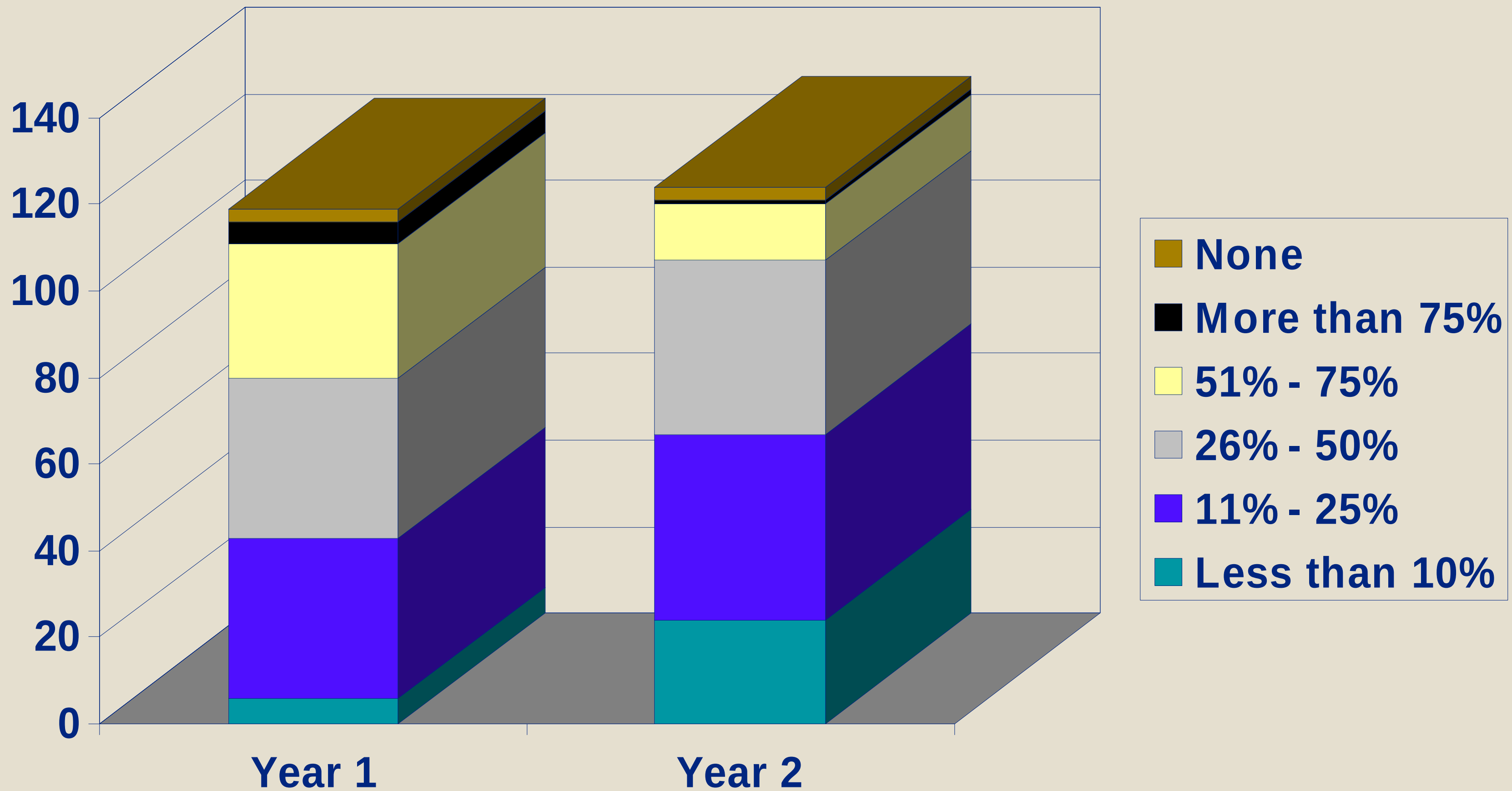
In analyzing both year 1 and year 2, what percentage of documentation and testing performed by your organization was unnecessary to provide reasonable assurance that your organization s internal control structure over financial reporting was effective?



In analyzing both year 1 and year 2, what percentage of documentation and testing performed by <u>your organization</u> was <u>unnecessary</u> to provide reasonable assurance that your organization s internal control structure over financial reporting was effective?

Topic	Less than 10%	11% - 25%	26% - 50%	51% - 75%	More than 75%	None	Not Answered
Year 1	10	30	45	29	7	0	10
Year 2	32	50	34	7	1	3	4

In analyzing both year 1 and year 2, what percentage of documentation and testing performed by the <u>external auditors</u> was <u>unnecessary</u> to provide reasonable assurance that your organization s internal control structure over financial reporting was effective?



In analyzing both year 1 and year 2, what percentage of documentation and testing performed by the <u>external auditors</u> was <u>unnecessary</u> to provide reasonable assurance that your organization s internal control structure over financial reporting was effective?

Topic	Less than 10%	11% - 25%	26% - 50%	51% - 75%	More than 75%	None	Not Answered
Year 1	6	37	37	31	5	3	12
Year 2	24	43	40	13	1	3	7

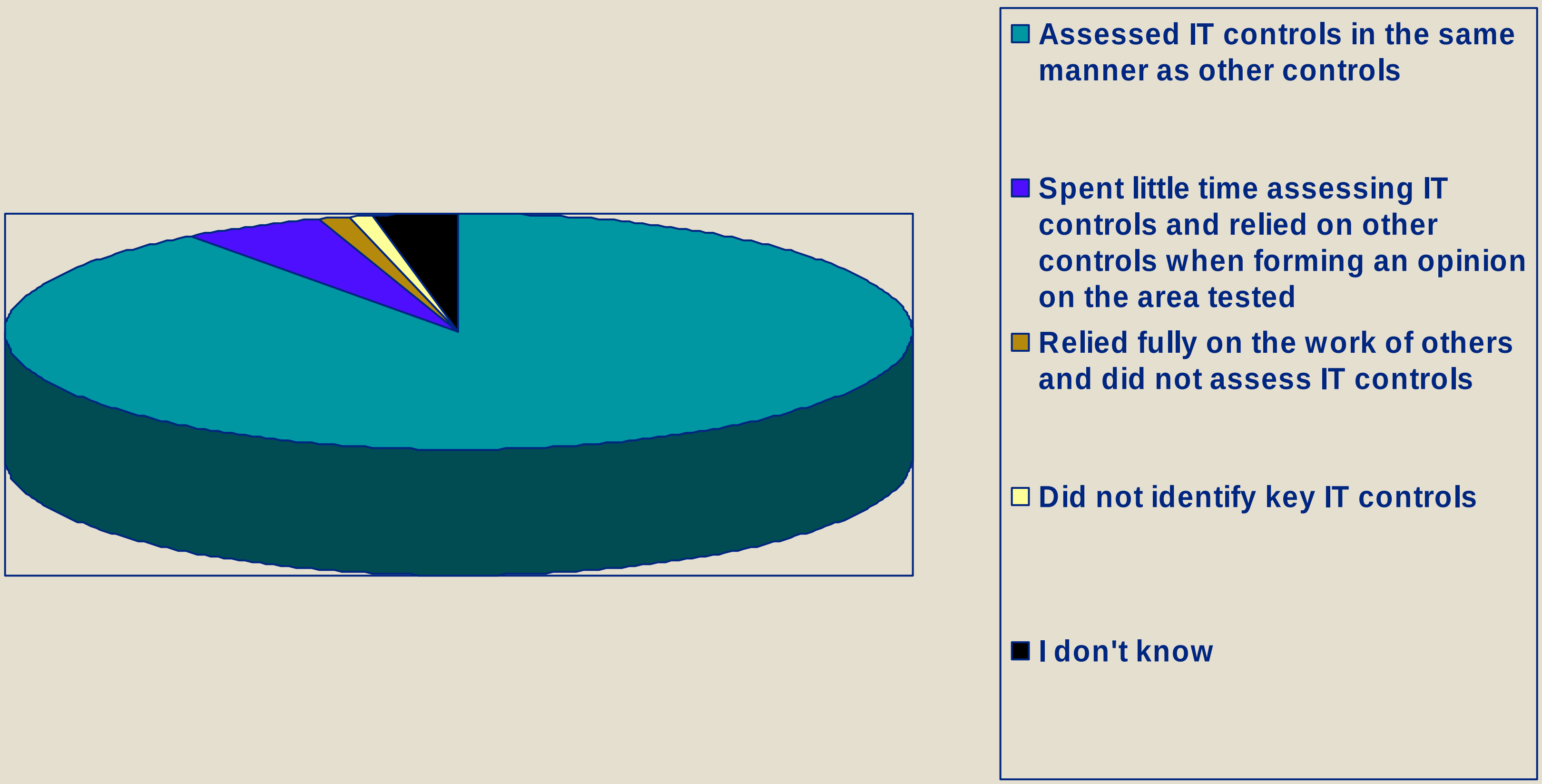
Please identify the percentage of responsibility for the completion of each task as performed by the different parties for year 1:

Task	External Providers	Internal Auditors	Process Owners / Mgmt.
Risk assessment	21%	45%	34%
Planning	25%	51%	24%
Documentation	23%	34%	43%
Planning	26%	60%	14%
Test plan	35%	51%	14%
Testing	31%	53%	16%
Identify Deficiencies	23%	55%	22%
Remediation action plan	11%	30%	59%
Testing of remediation	28%	57%	15%
Assessment of adequacy of ICFR	27%	46%	26%
Coordinating audit with external auditors	18%	52%	30%

Please identify the percentage of responsibility for the completion of each task as performed by the different parties for year 2:

Task	External Providers	Internal Auditors	Process Owners / Mgmt.
Risk assessment	13%	49%	38%
Planning	16%	56%	28%
Documentation	10%	34%	56%
Planning	17%	64%	19%
Test plan	27%	54%	19%
Testing	23%	57%	20%
Identify Deficiencies	17%	59%	24%
Remediation action plan	8%	29%	63%
Testing of remediation	20%	61%	19%
Assessment of adequacy of ICFR	20%	47%	33%
Coordinating audit with external auditors	14%	57%	29%

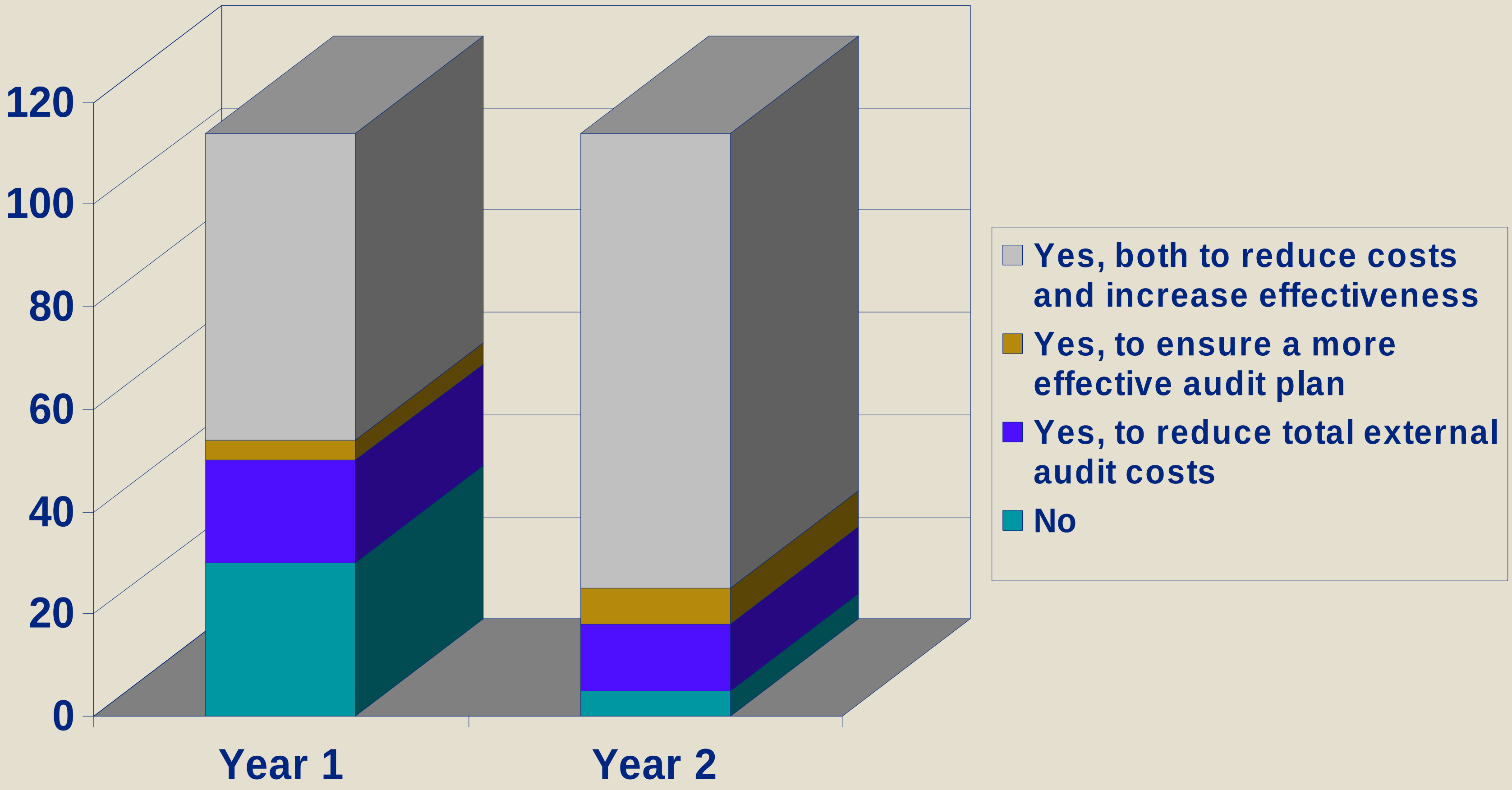
In your opinion, which of the following best describes external audit s testing of information technology controls in there §404 work?



In your opinion, which of the following best describes external audit s testing of information technology controls in there §404 work?

Choice	Count	Percentage of Sample Answering	Percentage of Total Sample
Assessed IT controls in the same manner as other controls	101	90.2%	77.1%
Spent little time assessing IT controls and relied on other controls when forming an opinion of the area tested	6	5.4%	4.6%
Relied fully on the work of others and did not assess IT controls	1	0.9%	0.8%
Did not identify key IT controls	1	0.9%	0.8%
I don't know	3	2.7%	2.3%

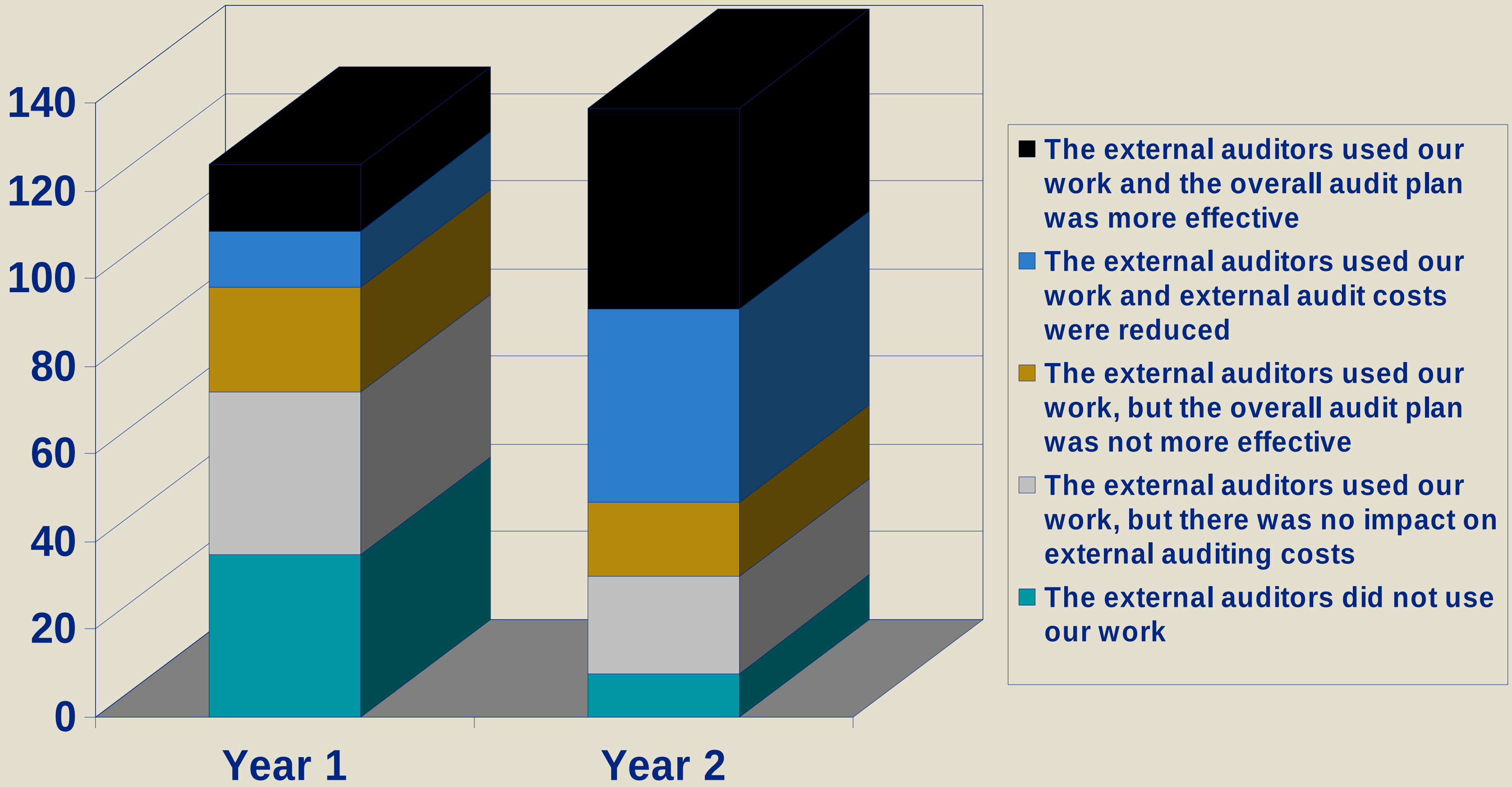
Analyzing year 1 and year 2, did the internal audit function within your organization complete work that could be used by the external auditors reduce their §404 work?



Analyzing year 1 and year 2, did the internal audit function within your organization complete work that could be used by the external auditors reduce their §404 work?

Topic	No	Yes, to reduce total external audit costs	Yes, to ensure a more effective audit plan	Yes, both to reduce costs and increase effectiveness	Not Answered
Year 1	30	20	4	60	17
Year 2	5	13	7	89	17

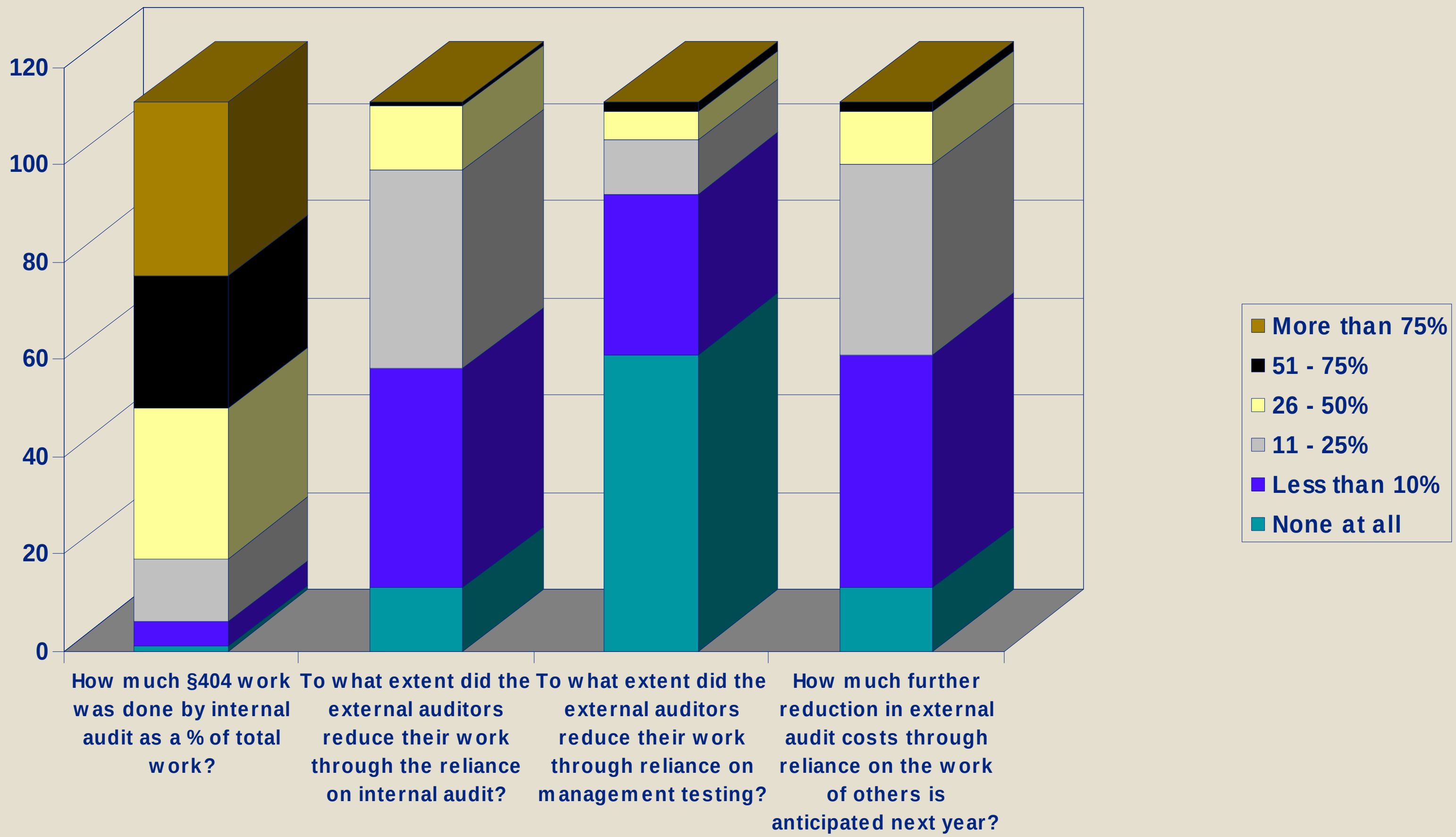
Analyzing year 1 and year 2, if you selected above that the internal audit function within your organization completed work that could be used by the external auditors to reduce their §404 work, please select how the work performed was used by the external auditors:



Analyzing year 1 and year 2, if you selected above that the internal audit function within your organization completed work that could be used by the external auditors to reduce their §404 work, please select how the work performed was used by the external auditors:

Topic	The external auditors did not use our work	The external auditors used our work, but there was no impact on external auditing costs	The external auditors used our work, but the overall audit plan was not more effective	The external auditors used our work and external audit costs were reduced	The external auditors used our work and the overall audit plan was more effective
Year 1	37	37	24	13	15
Year 2	10	22	17	44	46

Please answer the following questions:



Please answer the following questions:

Topic	None at all	Less than 10%	11 - 25%	26 - 50%	51 - 75%	More than 75%	No Answer
How much §404 work was done by internal audit as a percentage of their total work?	1	5	13	31	27	36	18
To what extent (percentage of total cost) did the external auditors reduce their work through their reliance on internal audit?	13	45	41	13	1	0	18
To what extent did the external auditors reduce their work through reliance on management testing performed by others outside of internal audit?	61	33	11	6	2	0	18
How much further reduction in external audit costs through reliance on the work of others is anticipated in the next year?	13	48	39	11	2	0	18

How strongly do you agree or disagree with the following statements?

Topic	Strongly disagree	Disagree	Neutral	Agree	Strongly agree	No basis for opinion
Our organization has clearly defined and identified the key controls	1	10	4	51	48	0
Our external auditors have clearly defined and identified the key controls	4	12	17	55	22	4
The definition and identification of key controls made by our organization and our external auditors was in agreement	2	19	14	50	25	4
If the key controls identified by management and the external auditors were not in agreement, the external auditors did not reconcile/agree their determined key controls with management s identified key controls	13	22	14	15	6	31

How strongly do you agree or disagree with the following statements?

Topic	Strongly disagree	Disagree	Neutral	Agree	Strongly agree	No basis for opinion
Our organization has effectively aligned key controls and significant risks within the organization	2	17	13	46	35	0
Our external auditors have effectively aligned key controls and significant risks within the organization	5	21	20	47	12	8
The alignment of key controls and significant risks as defined by our organization and the external auditors was in agreement	2	22	19	52	12	6
External auditors tested insignificant transactions or controls	3	11	13	49	33	3
External auditors tested entity-level controls before testing individual account controls	16	51	10	24	7	5

How strongly do you agree or disagree with the following statements?

Topic	Strongly disagree	Disagree	Neutral	Agree	Strongly agree	No basis for opinion
External auditors tested more controls than our organization believed was necessary	1	7	20	52	31	2
External auditors tested controls that did not relate to a risk-based approach and that could not materially impact the financial statements	1	19	14	53	23	2
External auditors performed separate tests for the purpose of the audit of internal controls and the financial statement audit	0	14	9	49	30	11
External auditors simplified their walkthroughs by following a single transaction through the entire process	2	16	21	44	10	20
External auditors utilized an appropriate methodology for selecting sample sizes	1	6	17	59	15	15
External auditors utilized appropriate testing methodologies	0	9	14	63	10	17

Average key controls identified comparing year 1 and year 2:

	YEAR 1	YEAR 2
Total key controls identified (104 responses)	85,683	67,593
Average key controls identified (104 responses)	824	650

21% decrease in identified key controls

How strongly do you agree or disagree with the following statements for year 1:

Topic	Strongly disagree	Disagree	Neutral	Agree	Strongly agree	No Answer
Management places importance on having strong corporate governance	0	1	11	39	59	21
Management places importance on having quality financial reporting	0	1	4	28	77	21
Management views the external auditors more favorably than the internal auditors in terms of trust, sharing information, or making oneself more readily available	21	47	29	12	2	20
Management encourages open communication and coordination with the external auditors	1	2	7	62	38	21
Management has a strong working relationship with the internal audit department	1	4	16	46	42	22
Management views the internal auditors more favorably than external auditors in terms of trust, sharing information, or making oneself more readily available	3	12	36	31	25	24
Management encourages open communication and coordination with the internal auditors	0	1	18	39	51	22

How strongly do you agree or disagree with the following statements for year 2:

Topic	Strongly disagree	Disagree	Neutral	Agree	Strongly agree	No Answer
Management places importance on having strong corporate governance	0	0	6	34	69	22
Management places importance on having quality financial reporting	0	0	2	26	81	22
Management views the external auditors more favorably than the internal auditors in terms of trust, sharing information, or making oneself more readily available	26	51	22	6	3	23
Management encourages open communication and coordination with the external auditors	0	2	7	59	41	22
Management has a strong working relationship with the internal audit department	0	1	5	53	49	23
Management views the internal auditors more favorably than external auditors in terms of trust, sharing information, or making oneself more readily available	2	8	28	38	30	25
Management encourages open communication and coordination with the internal auditors	0	1	7	41	58	24

How strongly do you agree or disagree with the following statements for year 1:

Topic	Strongly disagree	Disagree	Neutral	Agree	Strongly agree	No Answer
External auditors communicated all deficiencies to management in a timely manner	10	29	19	46	6	21
External auditors evaluated the adequacy of compensating controls when they identified a deficiency	6	26	27	46	5	21
Management concurred with the deficiencies identified by the external auditors	6	31	28	39	5	22
Management concurred with the means of resolution for the deficiencies identified by the external auditors	3	13	36	52	5	22
Management concurred with the external auditors regarding the disclosure of identified deficiencies	3	10	26	57	13	22
External auditors requested management s responses to deficiencies that were less than significant	10	16	11	51	20	23

How strongly do you agree or disagree with the following statements for year 2:

Topic	Strongly disagree	Disagree	Neutral	Agree	Strongly agree	No Answer
External auditors communicated all deficiencies to management in a timely manner	7	25	15	50	10	24
External auditors evaluated the adequacy of compensating controls when they identified a deficiency	3	21	23	51	9	24
Management concurred with the deficiencies identified by the external auditors	3	19	31	47	6	25
Management concurred with the means of resolution for the deficiencies identified by the external auditors	0	11	29	60	7	24
Management concurred with the external auditors regarding the disclosure of identified deficiencies	2	4	23	60	15	27
External auditors requested management s responses to deficiencies that were less than significant	9	21	11	44	20	26

Please provide additional comments if conflicts arose with your external auditors regarding identification, resolution, or disclosure of deficiencies:

This company had no material weaknesses or significant deficiencies in year 1 and none are expected for year 2.

Lease restatement automatically deemed to be a material weakness. Management disagreed but auditors held firm. Since then, PCAOB has stated that restatement does not automatically equal material weakness in ICOFR.

The neutral rating for mgmt concurrence with the deficiencies & the means of resolution is the result of both being a mixed bag --- a lot of agreement but with significant items of disagreement. Thus

External auditors are still focused on the materiality of the numbers involved and not the risk of a breakdown or misstatement in the processes.

The biggest complaint was that areas and accounts that our external auditor attested to in prior years were problematic for the same accounting treatment this year for SOX. This was a huge concern.

We disagreed on year 2 scope including accounting for leases which is a very insignificant activity and low risk for a misstatement for our company. However the external auditors' firm gave blanket instructions for all their engagements to assess controls over accounting for leases. Same was true for accounting for property plant and equipment. Final conclusion was the auditors agreed with our scope however have requested management to scope in these areas for year 3 for efficiencies for the external auditors. Consequently we believe the external auditors tested controls over low risk transactions.

Please provide additional comments if conflicts arose with your external auditors regarding identification, resolution, or disclosure of deficiencies (Continued):

Lacked Coordination. No two-way feedback.

PCAOB should offer guidance for resolving disputes between Management and the External Auditors.

Our external auditors designed a process to detect all, rather than material, deficiencies and expected remediation on everything.

Use gap evaluation framework version 3 published in December 2004

External auditors identified deficiencies no matter how slight they may have been

Management felt like it had to let the external auditor find a couple of "significant deficiencies" so they would finish.

The external auditors provided little input on deficiencies in Year 2 and relied almost entirely on management's interim and final conclusions in this area. I took this to mean they were in agreement with our internal approach and methodology for identifying, evaluating, and classifying deficiencies.

In the first year deficiencies noted by the external auditors were not communicated to management/internal auditors, but directly reported up. We were only informed that there were no material weaknesses noted. However, a number of control deficiencies were reported to the Audit Committee, which we considered unnecessary and inappropriate. In addition to a number of them management and internal audit disagree. We have discussed this with the auditors and they have promised improvement for this year. As our year-end is April 30, we do not have evidence of this, but expect it to improve. Therefore year 2 is set at neutral.

Please provide additional comments if conflicts arose with your external auditors regarding identification, resolution, or disclosure of deficiencies (Continued):

Evaluating significance of deficiencies

Year 1- management disagreed with the significance of 3 of 4 significant deficiencies identified by external auditors and stated so in letters to the audit committee. Year 2- Literally 5 minutes before final communications with the audit committee the external auditors classified a previously accepted practice as a significant deficiency, which management disagreed with.

Year one there were significant disagreements with external auditors over approach, testing, identification and evaluation of deficiencies. Their National Office was providing all guidance and it appeared that local office staff were just form filling. It tested the relationship, but in the end, the relationship previously established was critical to resolving all disagreements and coordinating a response or action plan.

We had deficiencies that we were able to prove had no material impact (or any impact) on the financial statements, yet the external auditors refused to remove them from the list. Two examples: "a garbage can is kept next to the printer in the computer room" and "the computer system processes information in batches as opposed to in real time". In both these cases, the external auditor was unable to explain why these were deficiencies.

Please provide additional comments if conflicts arose with your external auditors regarding identification, resolution, or disclosure of deficiencies (Continued):

The measurement of Balance Sheet dollar deficiencies vs. a Pre -tax income statement amount often leads to confusion as clearly immaterial Balance Sheet items (e.g.; reclasses) become an issue against a lower materiality.

I think there is some degree of risk to generic control expectations. The control is performed x way in other companies, therefore your control s/b the same. This is dangerous.

Our external audit firm dictated that we evaluate third party service auditors' exceptions found in their SAS 70 audit reports as deficiencies and determine if the exceptions were either deficiencies, significant deficiencies, or material weaknesses" in the company's internal control environment. The external audit firm made this request two days prior to our 10-K filing date in late February.

Twice we had situations where the auditor and the process owner believed they had identified the deficiencies (both in area of taxes, where auditors and clients must work closely together with data without the benefit of sequential sharing of data). In these cases, it was awkward to get to the bottom of it, as "who identifies" has an impact on the external auditor's view of internal controls at a client company.

Please provide additional comments if conflicts arose with your external auditors regarding identification, resolution, or disclosure of deficiencies (Continued):

Our external auditors attempted to force certain language in management's report on internal control that was less transparent than tht which management wanted. the company had to push for its language in the report.

This is very difficult....We did not officially disagree, because we were told to "Stop arguing, you're pissing me off". So we "concurred" with our auditors because to do otherwise would be suicide. Everyone is afraid to speak out because they live in fear of their audit firms. Our company has immature controls and had reported material weaknesses in 2004. We are very aware of our weak spots and had no illusions that our controls were fully effective. However, our external auditors pointed out areas as material weaknesses that were, in the judgment of our very experienced team, simply not materially likely to result in a misstatement in our financials. Discussions with colleagues has reinforced my view that we were held to an impossible standard in order to minimize the risk to our auditors, who were in mortal fear of a PCAOB audit. They were looking for controls that no company our size would have in place in areas that were extremely low risk. They also appeared to see no room between an A++ and an F - you either had every "model" control they had on their benchmark or it was a material weakness. I've never experienced anything like it and am seriously considering changing careers if this is what my job has become. A truly dreadful experience...

Please provide additional comments if conflicts arose with your external auditors regarding identification, resolution, or disclosure of deficiencies (Continued):

Initial conflicts that were resolved entailed how many and what types of deficiencies were lumped together to form a significant deficiency, especially in the IT area.

A material weakness was communicated very late in the process, making it impossible for management to remediate, let alone even adequately address the issue

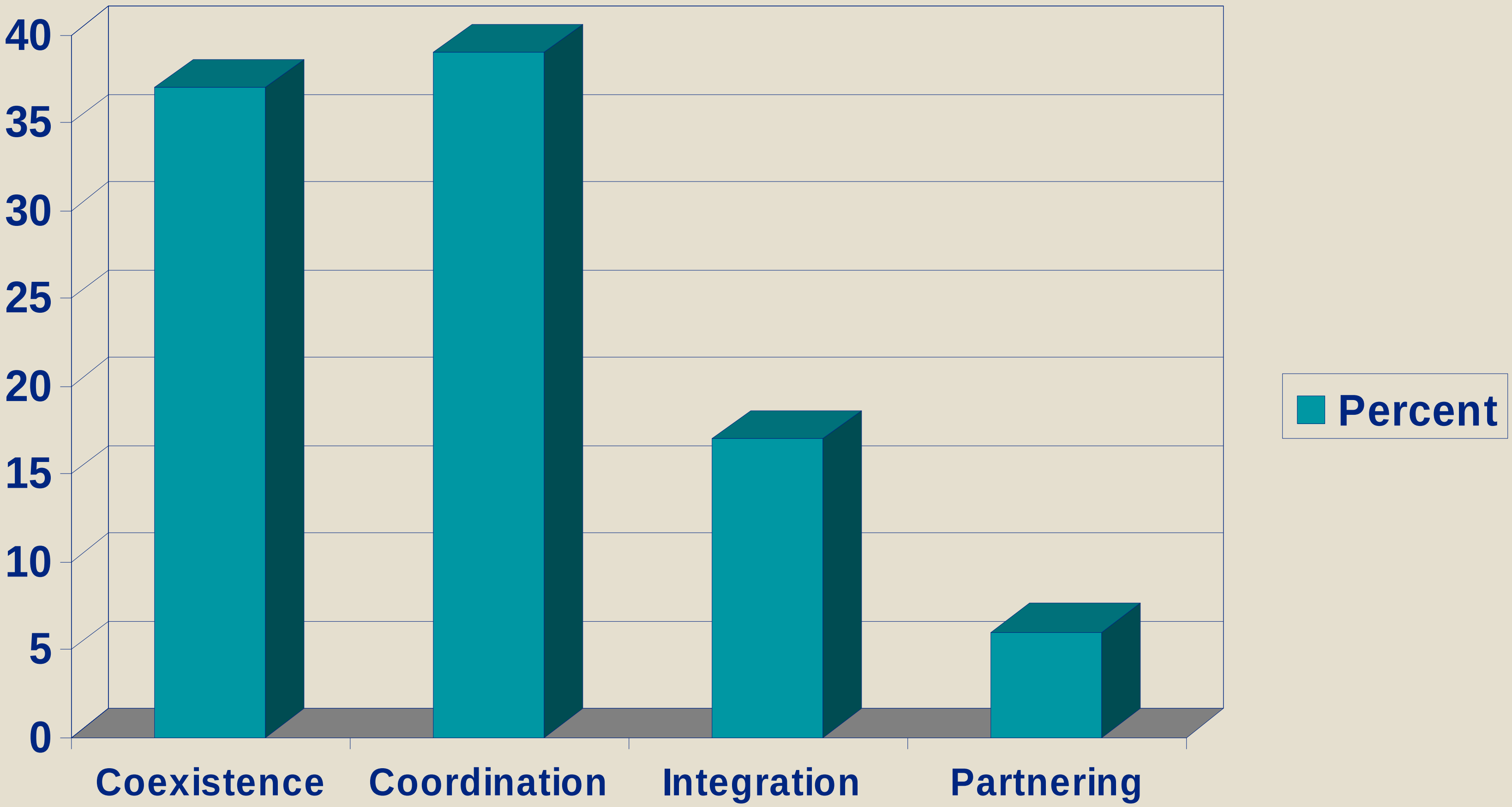
On some minor deficiencies clarification and understanding was needed to work through issues.

Since the PCOAB did not clarify testing on a timely basis the external auditors were very reluctant to provide any direction on number of controls, amount of testing etc.

We had no disclosures - but too much time spent documenting minor deficiencies (both internally and externally).

We had no deficiencies - but Mgmt would have fully cooperated with the External Auditors in assessing the deficiencies and immediately correcting. Also, in Year 1 the Internal Audit function was outsourced and towards the end of Year 2 it was co-sourced. Ongoing review of internal controls is most effective between Mgmt & Internal Audit - which then rubs on the independence factor. We have resorted to co-sourcing Internal Audit so that we have segregation of duty in this dual role of resource & test. Since External Audit independently performs all 404 test - the efforts are redundant. It's like cleaning your house before the housekeeper comes.

What was internal audit s relationship with the external auditors for year 1?



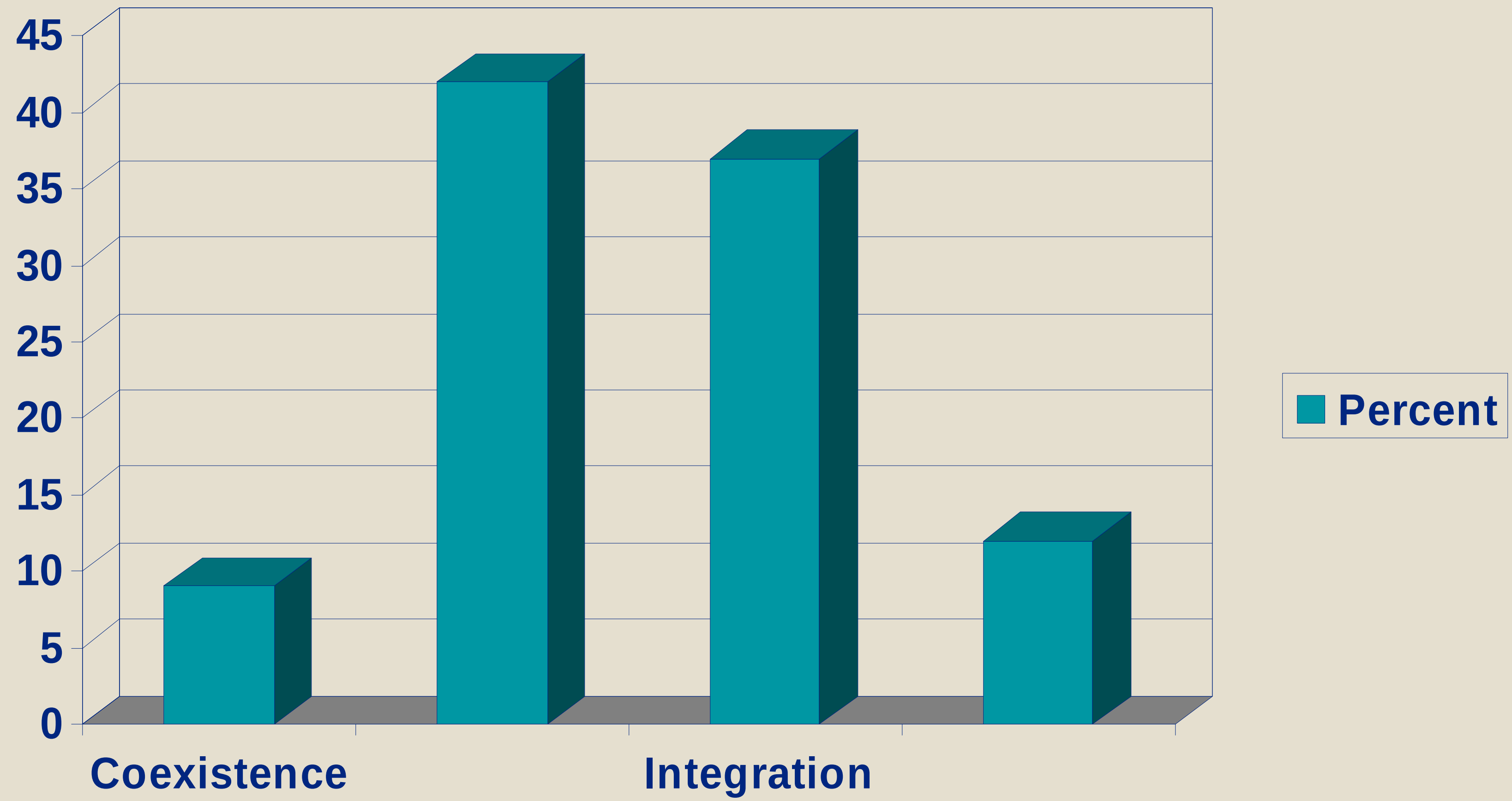
The Institute of Internal Auditors

Progress Through Sharing

What was internal audit s relationship with the external auditors for year 1?

Choice	Count	Percentage of Sample Answering	Percentage of Total Sample
Coexistence - perform separate and distinct activities with little interaction throughout the entire process	41	37.3%	31.3%
Coordination - independently develop but share information during the planning process with minor coordination on the development of audit plans	43	39.1%	32.8%
Integration - Risk assessment and audit plans are shared and external auditors rely on the work of internal audit, when applicable	19	17.3%	14.5%
Partnering - both parties have a shared and comprehensive goal regarding all aspects of the audit including defining corporate needs and expectations and the coverage of the audit encompassing financial, substantive, compliance, and systems auditing	7	6.4%	5.3%

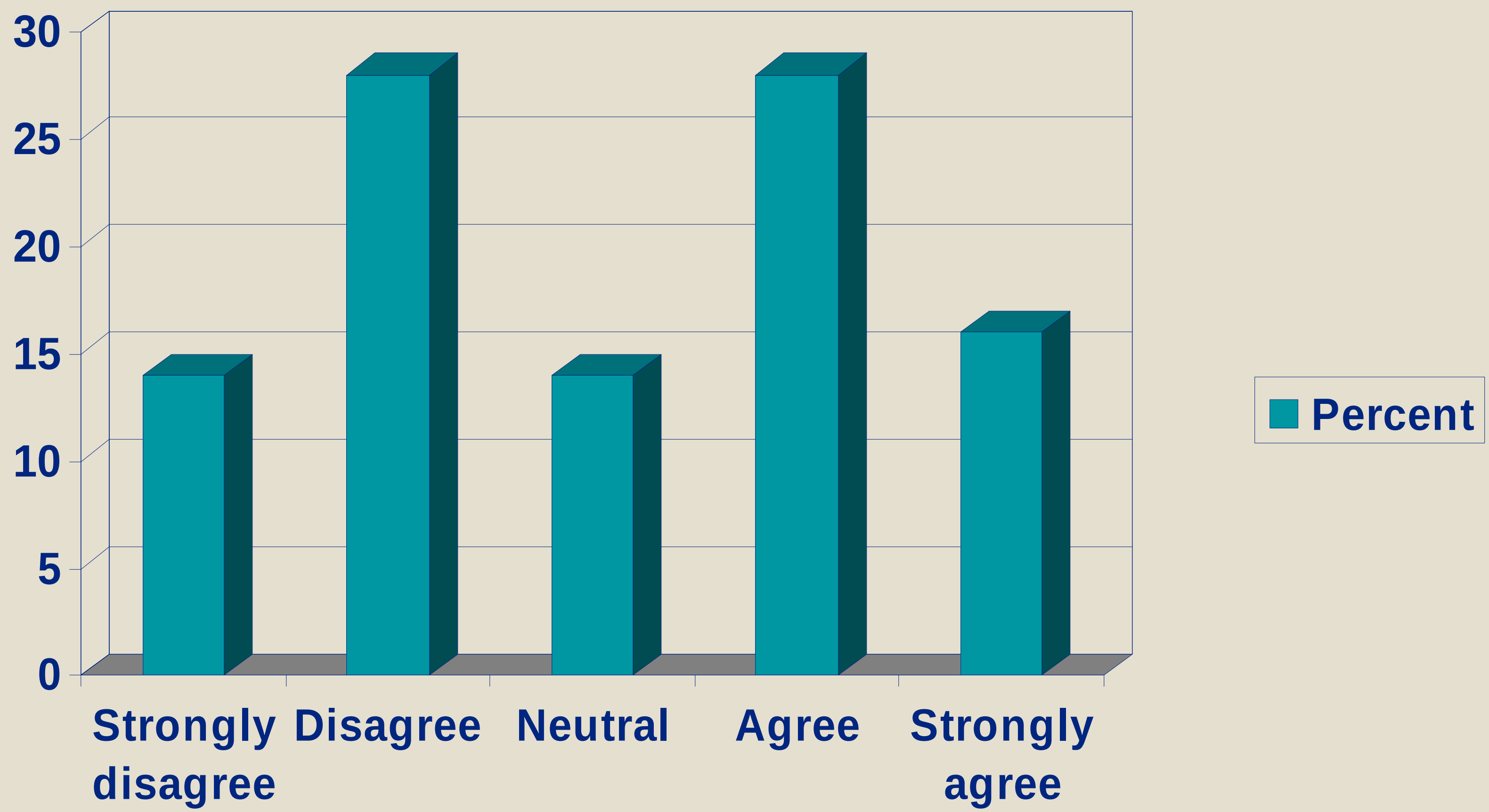
What was internal audit s relationship with the external auditors for year 2?



What was internal audit s relationship with the external auditors for year 2?

Choice	Count	Percentage of Sample Answering	Percentage of Total Sample
Coexistence - perform separate and distinct activities with little interaction throughout the entire process	10	9.1%	7.6%
Coordination - independently develop but share information during the planning process with minor coordination on the development of audit plans	46	41.8%	35.1%
Integration - Risk assessment and audit plans are shared and external auditors rely on the work of internal audit, when applicable	41	37.3%	31.3%
Partnering - both parties have a shared and comprehensive goal regarding all aspects of the audit including defining corporate needs and expectations and the coverage of the audit encompassing financial, substantive, compliance, and systems auditing	13	11.8%	9.9%

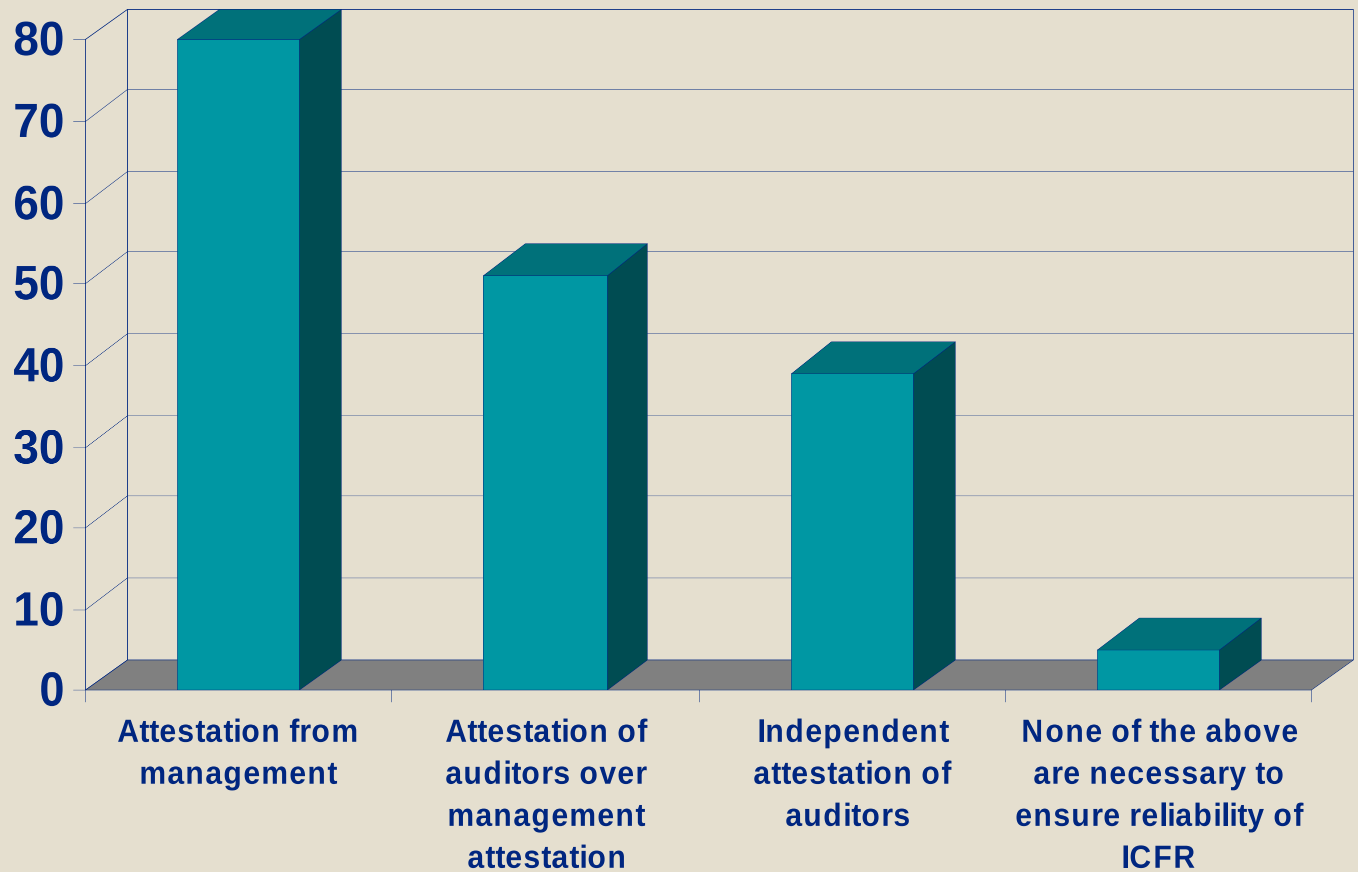
How strongly do you agree or disagree that the external auditor s opinion on management s annual certification of internal controls over financial reporting (ICFR) can be eliminated without lessening the reliability of management s annual certification?



How strongly do you agree or disagree that the external auditor s opinion on management s annual certification of internal controls over financial reporting (ICFR) can be eliminated without lessening the reliability of management s annual certification?

Choice	Count	Percentage of Sample Answering	Percentage of Sample Asked	Percentage of Total Sample
Strongly disagree	15	13.6%	11.5%	11.5%
Disagree	31	28.2%	23.7%	23.7%
Neutral	15	13.6%	11.5%	11.5%
Agree	31	28.2%	23.7%	23.7%
Strongly agree	18	16.4%	13.7%	13.7%

Currently, reporting on internal controls over financial reporting includes three attestations. Which combination of attestation(s) do you believe is the most appropriate and sufficient to ensure the reliability of ICFR?



Currently, reporting on internal controls over financial reporting includes three attestations. Which combination of attestation(s) do you believe is the most appropriate and sufficient to ensure the reliability of ICFR?

Choice	Count	Percent of Sample Asked	Percent of Total Sample
Attestation from management	80	61.1%	61.1%
Attestation of auditors over management attestation	51	38.9%	38.9%
Independent attestation of auditors	39	29.8%	29.8%
None of the above are necessary to ensure reliability of ICFR	5	3.8%	3.8%

Overall internal audit staff size for the following timeframes:

	Pre-SOX	YEAR 1	YEAR 2
Total auditors for all responses	1,179	1,413	1,582
Average staff size (81 respondents)	15.5	17.0	19.5

9.7% increase from Pre-SOX to Year 1

14.7% increase from Year 1 to Year 2

Please enter staff size comparisons for loaned or borrowed staff from other departments within the organization:

Role	Pre-SOX	Year 1	Year 2	Number of Responses
CAE	0.65	0.88	1	43
Audit Directors General	1.4	1.45	1.8	20
Audit Directors IT	0.86	1	1	8
Audit Directors Other Specialty	4	4.3	4.3	3
Audit Managers General	2.8	3.5	3.6	25
Audit Managers IT	0.94	1.25	1.5	16
Audit Managers Other Specialty	0.4	0.8	1	5
Audit Seniors/Staff General	4.9	7.1	7.3	42
Audit Seniors/Staff IT	1.08	1.7	2.3	25
Audit Seniors/Staff Other Specialty	0.5	1.4	2.2	17

For what specialty area did you loan or borrow staff from other departments within the organization?

Accounting

Finance

Finance staff at business units and corporate IT department

We fully outsource IA to a Big 4 firm. We have a Director of Internal Controls who manages the SOX process for management. System Owners are highly involved.

Transaction testing

Accounting and Finance   Information Technology

Finance

Finance, ISO Auditors, IT

IT

SOX dedicated - we are a small company and still technically do not have an internal audit department

For what specialty area did you loan or borrow staff from other departments within the organization? (Continued)

We pulled staff for general SOX work.

In year 1, we supplemented internal audit staff with external temporary resources.

Accounting trainees for testing purposes

Manufacturing, IT

people to be facilitators for SOX

The Controller has internally owned the SOX implementation and documentation; the IT Director has played a key role in documentation for that specialty area. Internal Audit was outsourced for the first two years and co-sourced (with one internal hire) at the end of the second year. The co-sourcing arrangement allowed for multiple resources and specialists.

IT

Information Technology

Accounting

Accounting

Assistance with documentation from all areas of company. ITGCC

Retail Operations (Loss Prevention); Selected Finance processes

IT

IT and language skills

IT, Treasury

IT

Please enter staff size comparisons for purchased staff from third-party providers:

Role	Pre-SOX	Year 1	Year 2	Number of Responses
CAE	0.5	1	0.83	6
Audit Directors General	0.13	1	0.73	15
Audit Directors IT	0	0.65	0.5	12
Audit Directors Other Specialty	0	1	0.67	3
Audit Managers General	0.3	2	1.5	29
Audit Managers IT	0.09	1.2	1	35
Audit Managers Other Specialty	0.3	2	1.3	3
Audit Seniors/Staff General	0.4	5.2	2.9	49
Audit Seniors/Staff IT	0.4	2	1.9	41
Audit Seniors/Staff Other Specialty	0.2	2.3	2.2	12

For what specialty area did you purchase services from third-party providers?

Testing IT
Accounting/Audit
General Computer controls testing
None
Testing of entity IT controls
Full outsourcing of IA function in all years.
Information Systems Consumer Lending
Business process
Internal Audit/IT audit
IT, ISO Auditors, Finance
IT Auditing
SOX auditors/analyst and director level "guidance"
Tax
SBA Sale of Assets and booking or gains.
IT Consultants for SAP Implementation

For what specialty area did you purchase services from third-party providers? (Continued)

n/a
Financial Reporting, Information Technology, General assistance
Financial Auditors
IT
IT + Telecom industry
IT review
Audit
IT
IT, International
ITGCC and assistance with ICFR testing
IT and Tax
TAX YR1
IT
SOX documentation
IT and language skills

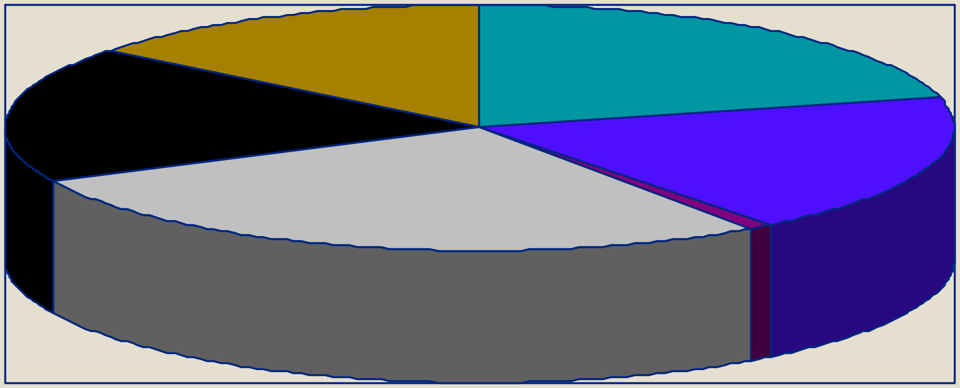
For what specialty area did you purchase services from third-party providers? (Continued)

IT
IT
IT
none
We didn't
IT
no purchased staff
IT, Governance
KPMG
IT General Controls and Testing
Internal auditing
Tax   IT
None
General auditing. Contractor asistance due to employee leave of absence.
General Process Documentation   IT

For what specialty area did you purchase services from third-party providers? (Continued)

project management consulting
IT
All SOX work
Operations (billing)
IT
IT and Nevada Gaming Compliance
404 Control Reviews
IT General Controls

How did your external auditors bill your organization for the annual financial statement audit?



- Separate billings for §404 work and the financial statement audit both at a fixed fee.
- Separate billings for §404 work and the financial statement audit both at a variable fee.
- Separate billings with §404 work billed at a fixed fee and the financial statement audit billed at a variable rate.
- Separate billings with §404 work billed at a variable rate and the financial statement audit billed at a fixed fee.
- Combined billing at a fixed fee
- Combined billing at a variable rate

The Institute of Internal Auditors

Progress Through Sharing

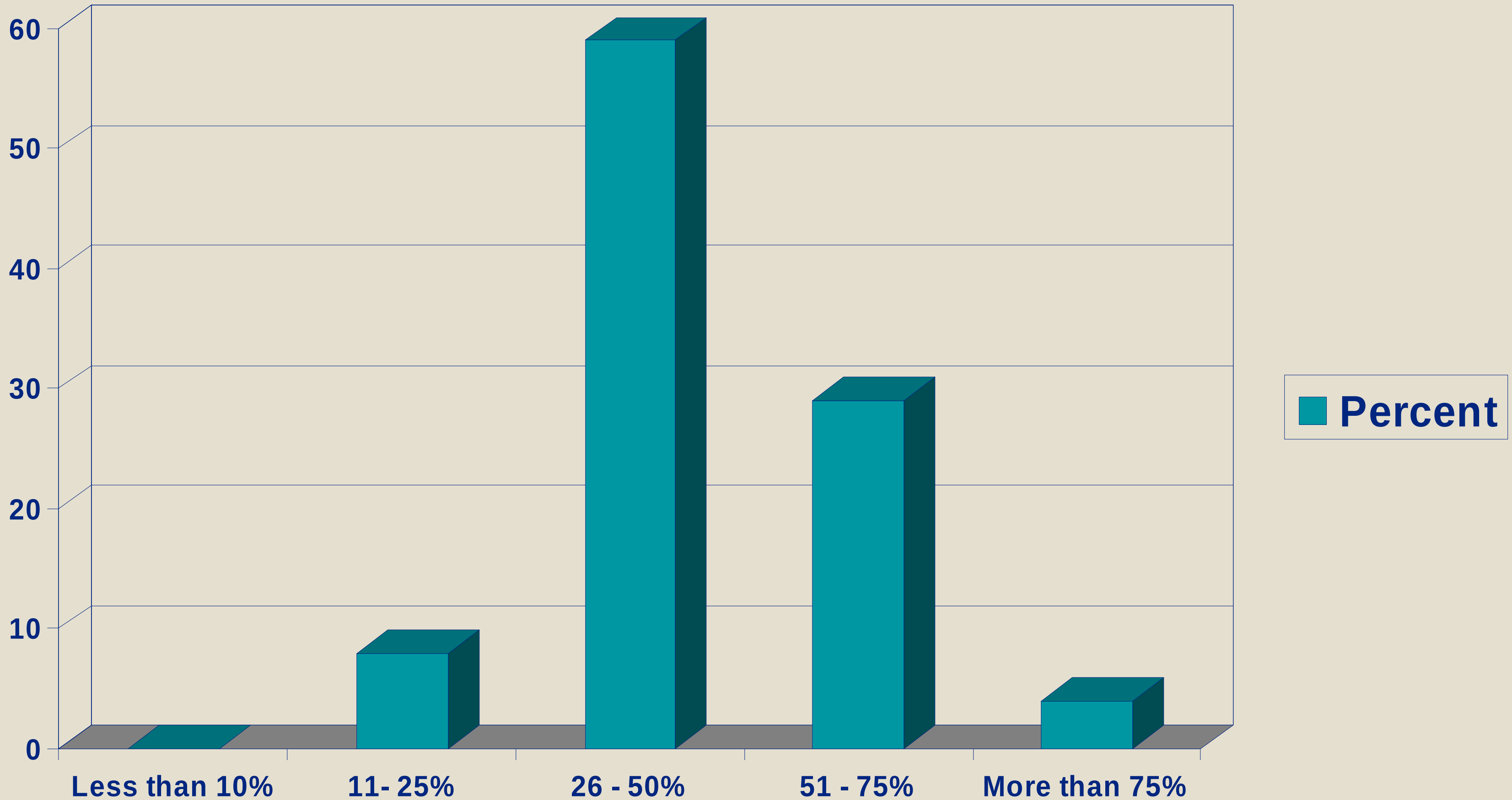
How did your external auditors bill your organization for the annual financial statement audit?

Choice	Count	Percentage of Sample Answering	Percentage of Total Sample
Separate billings for §404 work and the financial statement audit with both at a fixed fee	22	21.2%	16.8%
Separate billings for §404 work and the financial statement audit with both at a variable rate	19	18.3%	14.5%
Separate billings with §404 work billed at a fixed fee and the financial statement audit billed at a variable rate	1	1.0%	0.8%
Separate billings with §404 work billed at a variable rate and the financial statement audit billed at a fixed fee	28	26.9%	21.4%
Combined billing at a fixed fee	19	18.3%	14.5%
Combined billing at a variable rate	15	14.4%	11.5%

What were your organization s total external audit fees (financial statement audit and §404)

	Pre-SOX	Year 1	Year 2
Total fees	$181,751,348	$351,461,515	$317,242,090
Average Fees	$2,271,892	$3,820,234	$3,486,177
Number of Responses	80	92	91

What percentage of your organization s total external audit fees related to §404 costs in year 2?



What percentage of your organization s total external audit fees related to §404 costs in year 2?

Choice	Count	Percentage of Sample Answering	Percentage of Sample Asked	Percentage of Total Sample
Less than 10%	0	0.0%	0.0%	0.0%
11 - 25%	8	8.1%	6.1%	6.1%
26 - 50%	58	58.6%	44.3%	44.3%
51 - 75%	29	29.3%	22.1%	22.1%
More than 75%	4	4.0%	3.1%	3.1%

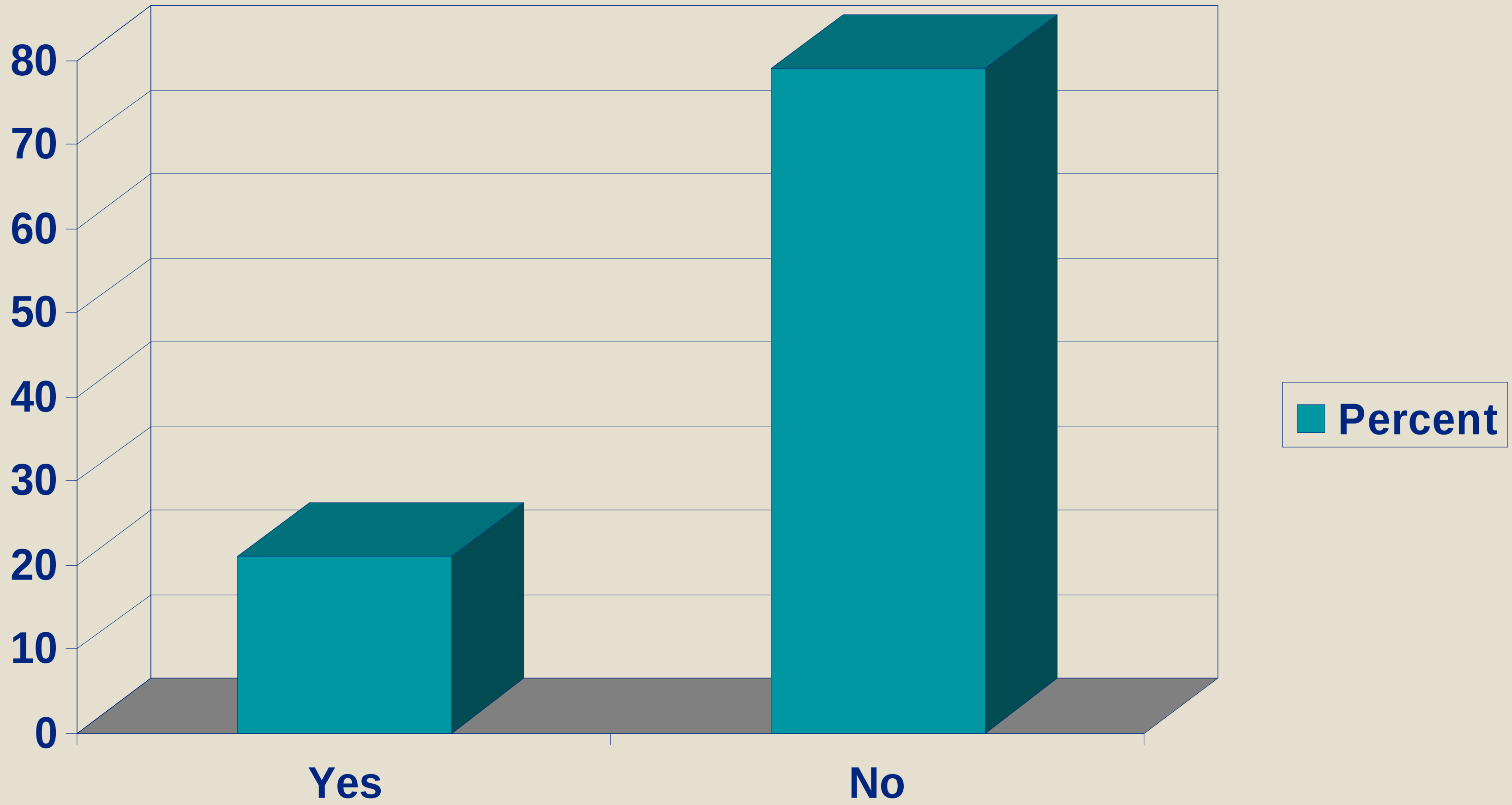
What percentage of total §404 costs (internal and external) were related to:

	% of costs
External Audit Fees	55%
Internal audit costs (internal and external)	34%
Third-party services not managed by internal audit	6%
Other	5%

Please specify the others areas that made up total §404 costs:

Tax assistance
Internal costs - Director of Internal Control, Business Information Office, System Owners
Process Owner time
Developed dedicated SOX audit department during Year 2
Accounting oversight of 3rd party services not managed by internal audit
Operational Management and Staff time
Management time to understand testing and conduct their assessments of the controls.
Process owner internal costs
Separate SOX function and many other Sox teams throughout the organization
Finance employee time
Controller's organization
Management's self testing
Internal Controls dept staff
Internal Auditor hired; use of local public firm managed by internal audit
Management efforts directed to compliance
Business areas

Did you see an increase in any other audit services in year 2 over year 1?



Did you see an increase in any other audit services in year 2 over year 1?

Choice	Count	Percentage of Sample Answering	Percentage of Sample Asked	Percentage of Total Sample
Yes (specified below)	21	20.8%	16.0%	16.0%
No	80	79.2%	61.1%	61.1%

Please specify what other services you experienced an increase in costs?

Tax

third party assistance for tax work

external auditors significantly modified there FS audit approach and performed many more procedures.

Tax

404 and financial statements

tax

Tax

Tax

Tax

tax

Additional entities to be audited.

Tax

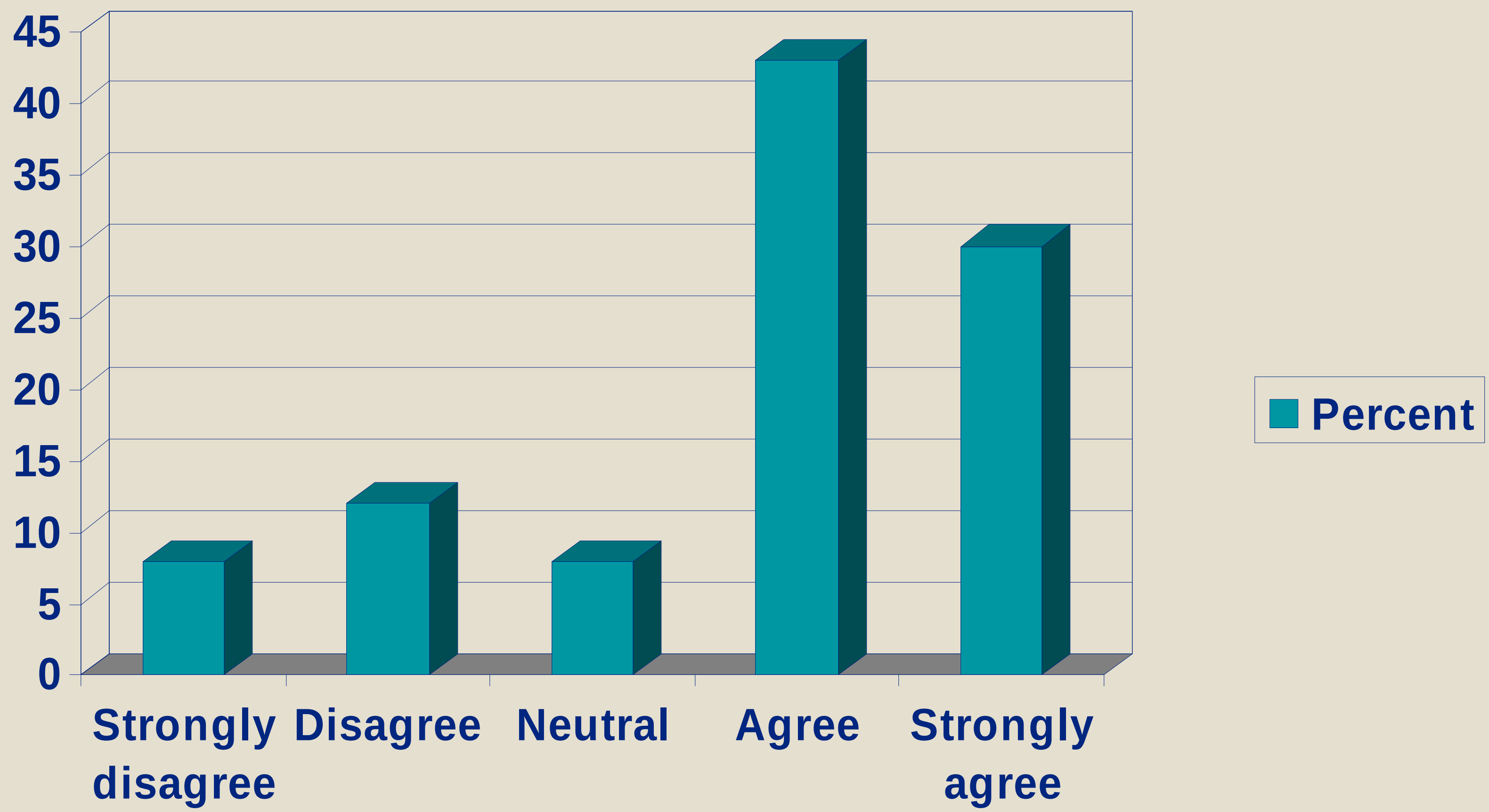
Tax

tax

Please specify what other services you experienced an increase in costs? (Continued)

other regulatory compliance and directors liability areas
tax compliance
tax FAS109 related issues
Divestitures and Joint Venture partnerships
Tax, subsidiary SOX compliance
relative to controls over the reporting of tax

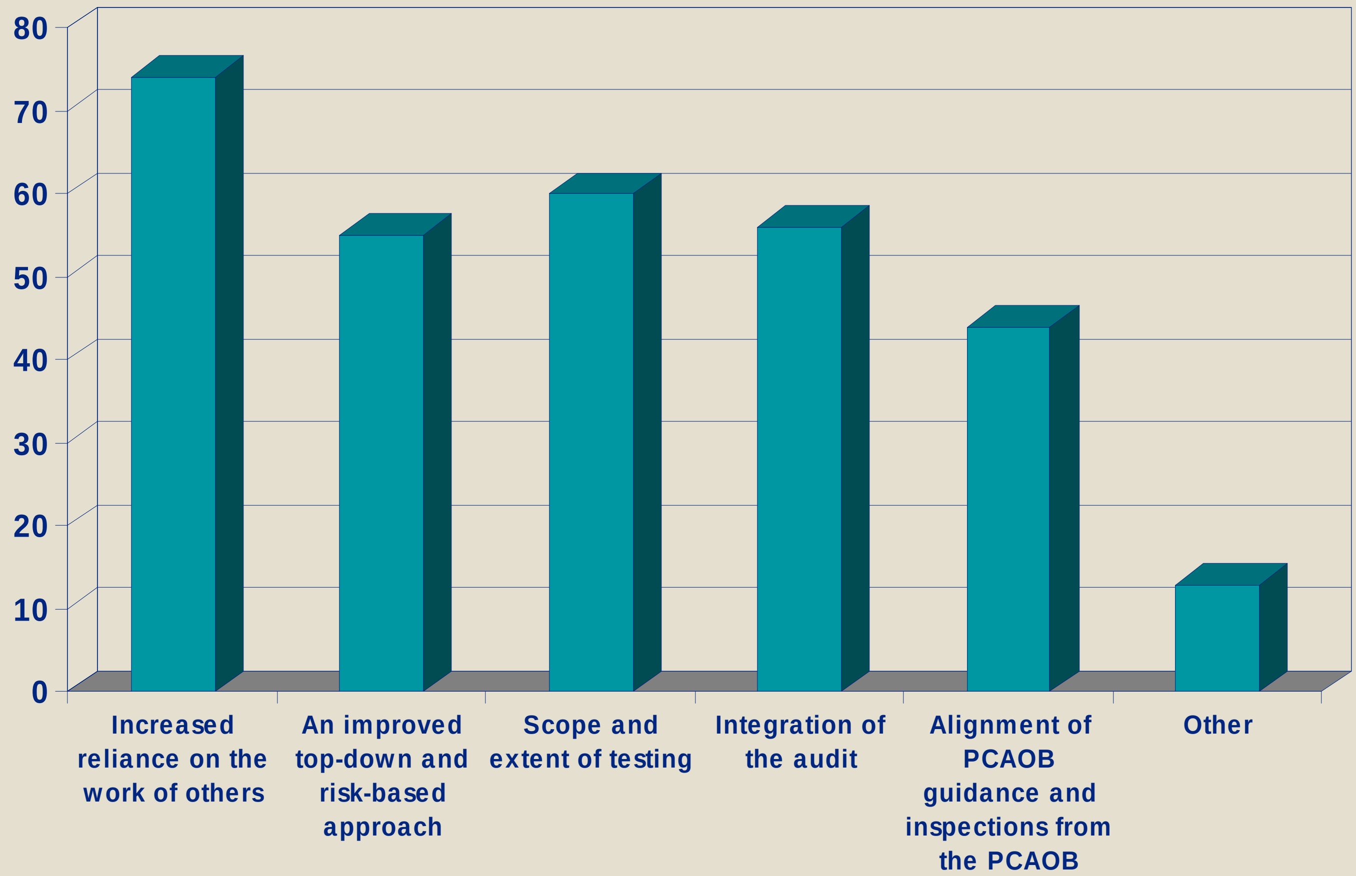
How strongly do you agree or disagree that a significant reduction in external audit costs related to §404 work can be achieved?



How strongly do you agree or disagree that a significant reduction in external audit costs related to §404 work can be achieved?

Choice	Count	Percentage of Sample Answering	Percentage of Sample Asked	Percentage of Total Sample
Strongly disagree	8	7.7%	6.1%	6.1%
Disagree	12	11.5%	9.2%	9.2%
Neutral	8	7.7%	6.1%	6.1%
Agree	45	43.3%	34.4%	34.4%
Strongly agree	31	29.8%	23.7%	23.7%

If you believe that a significant reduction in external audit costs can be achieved, will the major driver of this reduction be:



If you believe that a significant reduction in external audit costs can be achieved, will the major driver of this reduction be:

Choice	Count	Percent of Sample Asked	Percent of Total Sample
Increased reliance on the work of others	74	56.5%	56.5%
An improved top-down and risk-based approach	55	42.0%	42.0%
Scope and extent of testing	60	45.8%	45.8%
Integration of the audit	56	42.7%	42.7%
Alignment of PCAOB guidance and inspections from the PCAOB	44	33.6%	33.6%
Other; please specify areas for future cost reduction:	13	9.9%	9.9%

If you believe that a significant reduction in external audit costs can be achieved, what will other major drivers of this reduction be?

Reduction of the "Big 4" firms' monopoly status which inflates billing rates enormously.

All of these things would have to happen, but we do not believe they will. National offices of Big 4 firms are imposing requirements that will not facilitate.

Improved rationalization of company's designated key controls

Basic supply and demand of due to the lack of resources in the nation! variable rates increase 20% a year for the past two years

Historical perspective/reliance verses 100% retesting each year

Improved documentation supporting financial controls and financials

COMMON SENSE

experience and less fear by external auditors of being censured by the PCAOB

Scope and extent of testing needs to change for BOTH external and internal audit

common sense

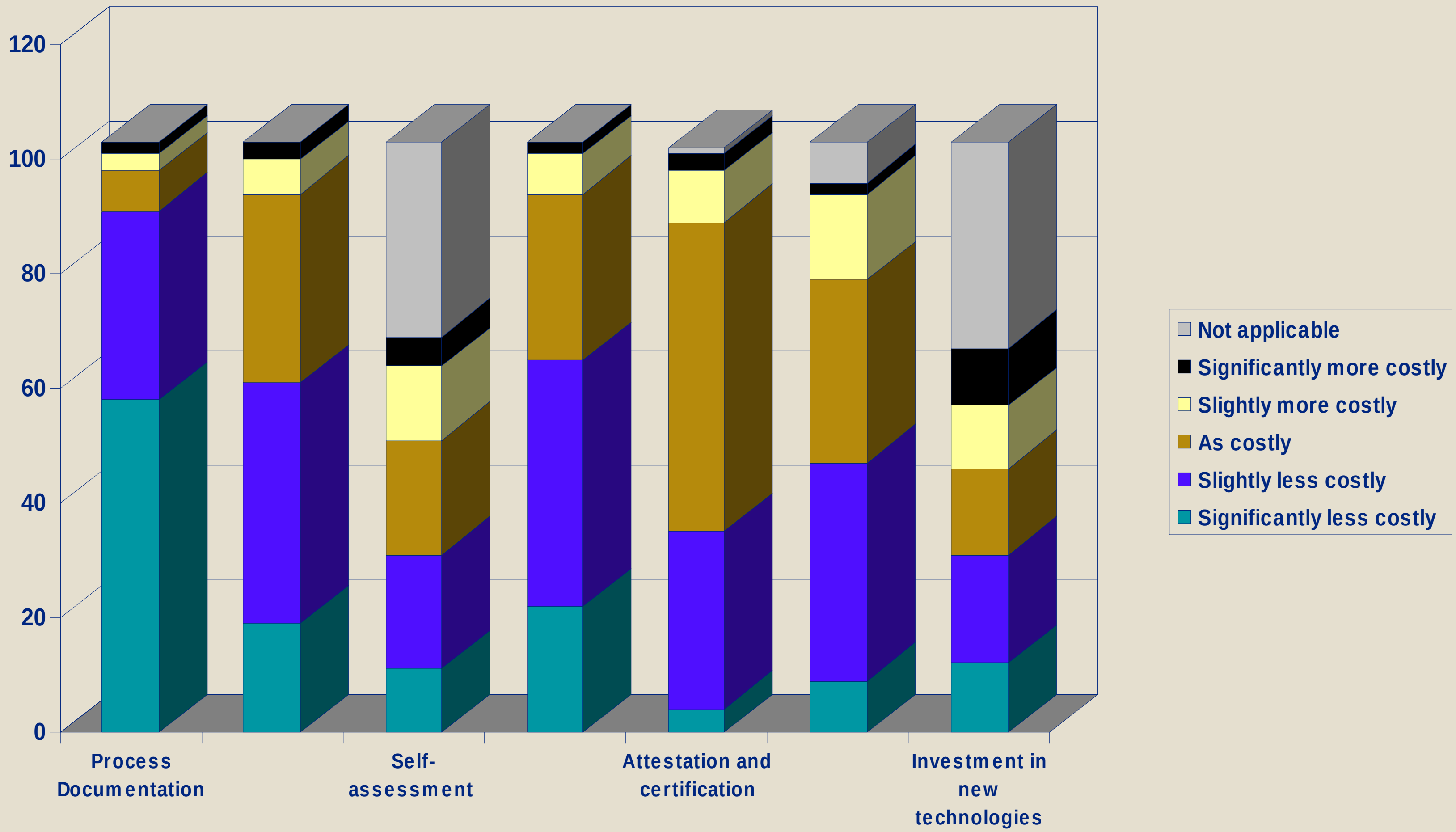
Eliminate attestation of management's report on controls.

External Audit seems firm in their approach, with inconsistencies within an audit firm in regards to implementation of any of the listed process improvements.

Costs will be reduced only if the 404 requirements are more tightly defined

Willingness of the partner to accept a lower number of hours (they beat the h--- out of this work).

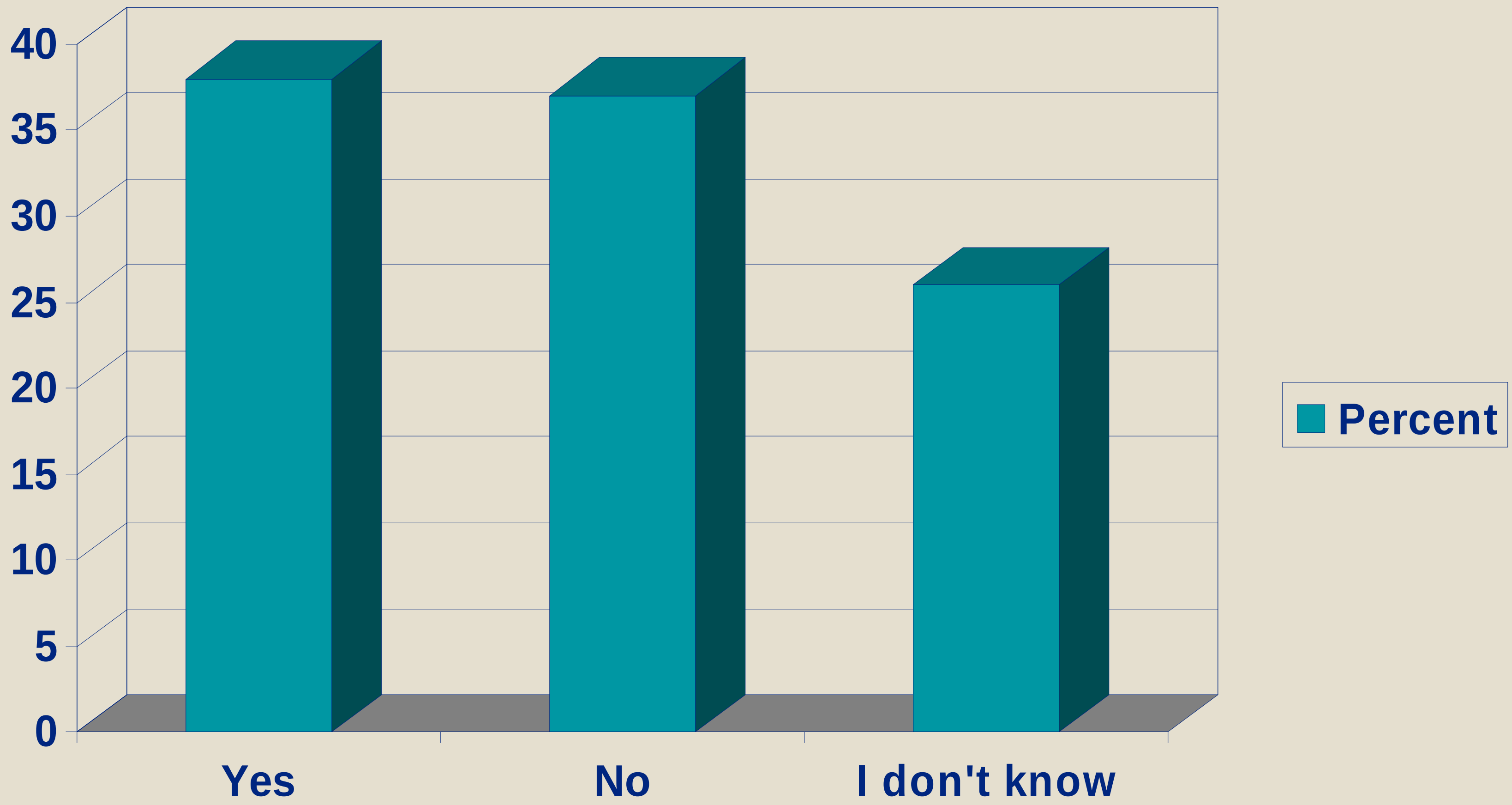
Please identify whether these activities were more or less costly to your organization with regards to year 2 compliance as compared to year 1:



Please identify whether these activities were more or less costly to your organization with regards to year 2 compliance as compared to year 1:

Topic	Significantly less costly	Slightly less costly	As costly	Slightly more costly	Significantly more costly	Not applicable
Creating and maintaining process documentation	58	33	7	3	2	0
Testing of key controls	19	42	33	6	3	0
Self-assessment by process owners	11	20	20	13	5	34
Remediation related activities	22	43	29	7	2	0
Attestation and certification	4	31	54	9	3	1
Staff training	9	38	32	15	2	7
Investment in new tools and technologies	12	19	15	11	10	36

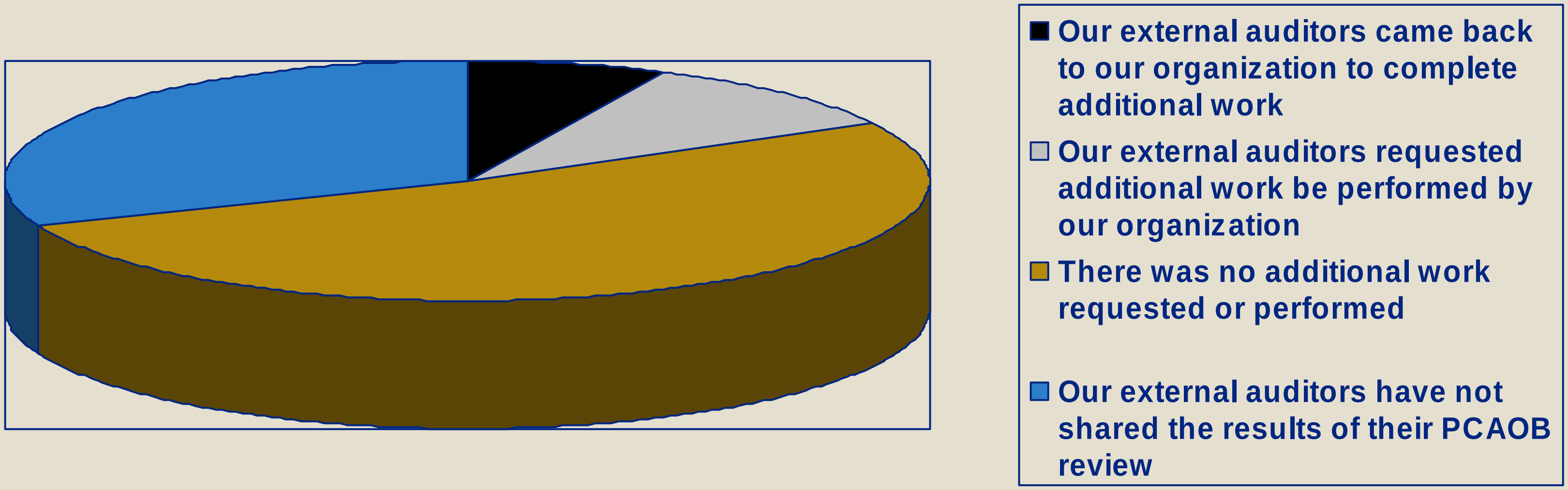
Has your external auditor's §404 work been examined by the PCAOB?



Has your external auditor's §404 work been examined by the PCAOB?

Choice	Count	Percentage of Sample Answering	Percentage of Sample Asked	Percentage of Total Sample
Yes	39	37.5%	29.8%	29.8%
No	38	36.5%	29.0%	29.0%
I don t know	27	26.0%	20.6%	20.6%

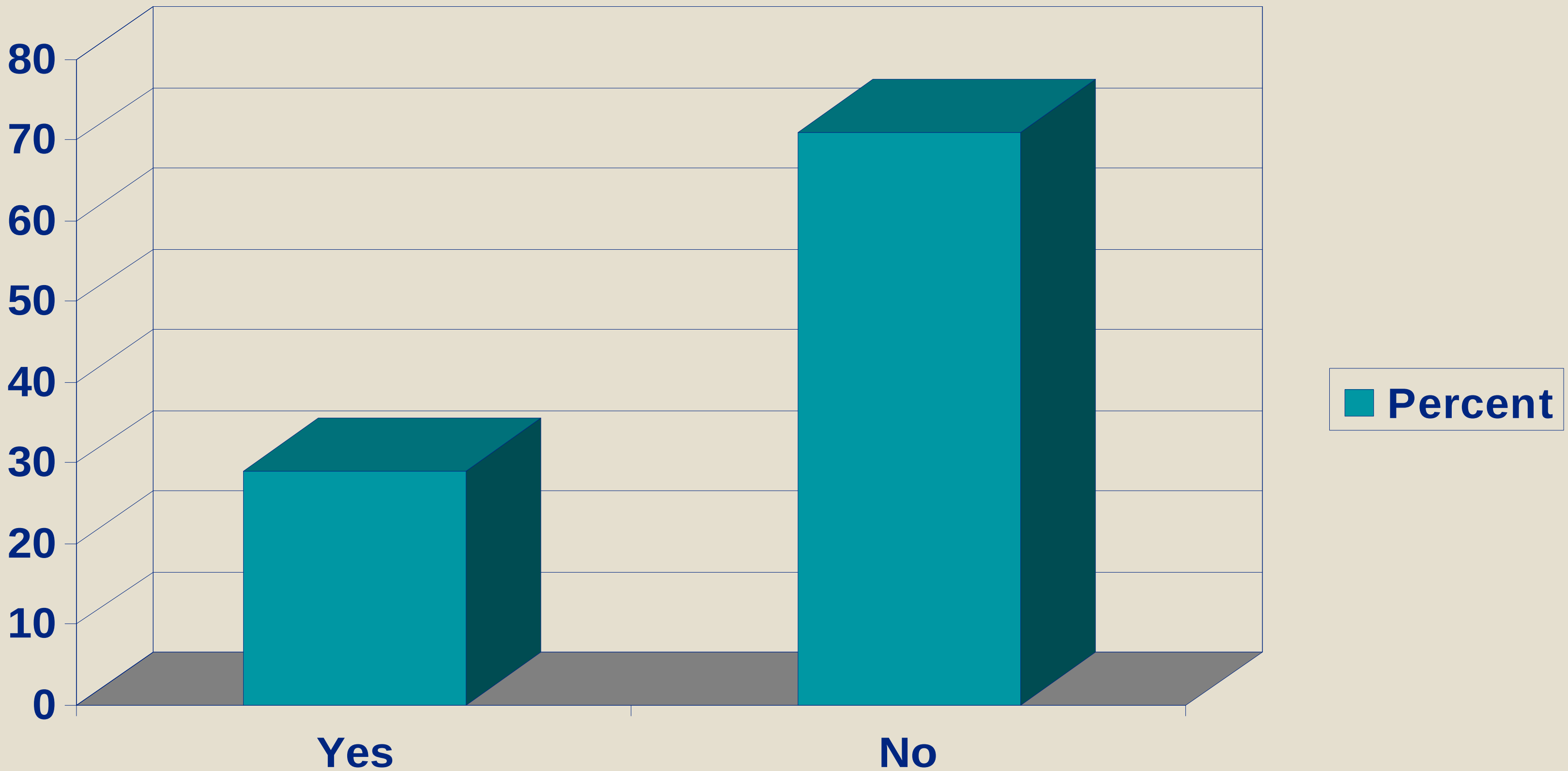
If your external auditor's §404 work was reviewed by the PCAOB, what was the outcome of this review?



If your external auditor's §404 work was reviewed by the PCAOB, what was the outcome of this review?

Choice	Count	Percentage of Sample Answering	Percentage of Sample Asked	Percentage of Total Sample
Our external auditors came back to our organization to complete additional work	3	7.1%	2.3%	2.3%
Our external auditors requested additional work be performed by our organization	4	9.5%	3.1%	3.1%
There was no additional work requested or performed	22	52.4%	16.8%	16.8%
Our external auditors have not shared the results of their PCAOB review	13	31.0%	9.9%	9.9%

If your external auditor's §404 work was reviewed by the PCAOB, has your external auditor indicated that a gap exists between the principles in PCAOB guidance and their review of the external auditor's §404 work?



If your external auditor's §404 work was reviewed by the PCAOB, has your external auditor indicated that a gap exists between the principles in PCAOB guidance and their review of the external auditor's §404 work?

Choice	Count	Percentage of Sample Answering	Percentage of Sample Asked	Percentage of Total Sample
Yes	12	28.6%	9.2%	9.2%
No	30	71.4%	22.9%	22.9%

If your external auditor's §404 work was reviewed by the PCAOB, how strongly do you agree or disagree that a gap exists between the principles in PCAOB guidance and their review of the external auditor's §404 work?

Choice	Count	Percentage of Sample Answering	Percentage of Sample Asked	Percentage of Total Sample
Strongly disagree	2	4.2%	1.5%	1.5%
Disagree	3	6.3%	2.3%	2.3%
Neutral	12	25.0%	9.2%	9.2%
Agree	7	14.6%	5.3%	5.3%
Strongly agree	10	20.8%	7.6%	7.6%
No basis for opinion	14	29.2%	10.7%	10.7%

In your opinion, what impact do you believe the PCAOB's oversight reviews have had on your external auditor?

Choice	Count	Percentage of Sample Answering	Percentage of Total Sample
No impact	19	19.4%	14.5%
Improved adherence to top-down, risk-based audit principles outlined in the March 16th 2005 PCAOB questions and answers	16	16.3%	12.2%
Decreased adherence to top-down, risk-based audit principles outlined into he March 16th 2005 PCAOB questions and answers	28	28.6%	21.4%
I don't know	35	35.7%	26.7%

Please take a moment to identify any key §404 topics not addressed in this survey or additional comments you would like to share:

I think it is important to understand that the assignment of professional internal auditors to major compliance-driven testing activities that have little chance of uncovering financial reporting problems or fraud and thereby reducing work that does uncover financial reporting problems results in a reduction in the reliability of financial reporting. Much of the useless testing work in this organization is driven by external auditor enforced rules that seem to be in conflict with the very reasonable May 16 guidance.

This is more of a PCAOB issue than IIA, but some entity should study how much the external audit firms (Big Four) have increased hourly rates in the last five years.

PCAOB guidance allows base-lining application control, however, virtually no company could meet the rigor of the guidance provided by the Big 4 and were not able to baseline. Defining a significant location at a 5% bright-line is not risk based. There should be a level where qualitative factors are considered - say 4-8%. Guidance is contradictory in requiring testing of where transactions originate and top down approach. Therefore spend way too much time testing AP and payroll transactions. Big 4 are afraid to be risk based for fear of PCAOB nitpicking.

Please take a moment to identify any key §404 topics not addressed in this survey or additional comments you would like to share: (Continued)

Further guidance on IT risks and controls from the PCAOB.

We need to do a better job in identifying the scope of what needs to be done from a control standpoint and better integrate this into the AUDIT process as a hole and not just as it relates to financial reporting. Other audit issues exists that are getting lost!

All companies are still struggling due to the lack of concrete guidance for management. It is a extremely serious flaw that guidance only exists for the auditors. Also COSO for small public companies is not feasible. Small companies generally don't have the caliber of resources to read and let allow implement the theoretical 200+ page small company draft issued by COSO - most of us just thought here we go again. One other comment...your demographic question below on company size typifies how smaller companies issues are not readily considered. Why group 100-500 million? That's a huge range with hugely different risks and infrastructures. It feels like you are really only looking for the big guys input

The external auditors despite their challenges with the PCAOB have taken advantage of the situation to increase and maintain profit margins by increasing both rate and hours.

Please take a moment to identify any key §404 topics not addressed in this survey or additional comments you would like to share: (Continued)

Questionnaire did not seem to allow for entities that formed a SOX compliance group independent of IA.

The external auditors still do not adequately integrate the two pieces of the audit. The auditors still audit for deficiencies rather than material weaknesses.

It appears the PCAOB guidance is ignored by the PCAOB inspectors in their inspections.

Need more guidance and specific examples on how to leverage results of entity-wide controls testing to help reduce nature, timing, and extent of substantive testing in process areas.

Asking opinion about whether we believe whether 404 as in the Sarbanes Oxley Act has been properly translated into guidance by the SEC and PCAOB to assure that it meets its objective. I think it does not meet that objective, it is a paper tiger, which leads to 'fake assurance' for the investor. The future may prove this after which the (external) audit profession will end up in a total disarray. Other ways will need to be found to achieve the objectives, such as force training on management, force auditors away from sales and profits only, but regain their professional attitude and integrity!

SOX section 302 and penalties are very appropriate. Keep External Auditor work and S404 minimized - adds no value.

Please take a moment to identify any key §404 topics not addressed in this survey or additional comments you would like to share: (Continued)

Once a Company complies with S404 for the first time - all low and medium (i.e. non-high) risk controls should be put on a 3 year ROTATION. High risk controls should still be tested each year - but there is very little value to the other 50-75% of the testing (especially after year one). This is similar to the "maturity factor" theory published by Protiviti which suggests there should be a rotation or reduced sample for controls that test without exception for consecutive years. Each year, documenting and testing these controls will offer less and less value ... the current approach is not sustainable. Also - there needs to be a better way of measuring control environment ... and making a specific and tangible translation of a strong control environment into less detailed scope and testing. It sounds good in theory - but it is very difficult in practice, since the external auditors are so attached to their control frameworks. Lastly - while management could easily make decisions to eliminate certain controls from the framework - the external auditors hold the cards since they can subsequently state that either A) they will need to still test it themselves (at expensive rates); or B) they will not be comfortable with management's attestation process. We are at their mercy ... even though MANAGEMENT should be driving the bus (since we really understand the risks and controls the best).

Please take a moment to identify any key §404 topics not addressed in this survey or additional comments you would like to share: (Continued)

Spreadsheet testing is out of proportion to other control tests   Excessive focus on signatory controls   Insignificant reliance on management's testing   Inadequate assessment of the total suite or inventory of process controls compared to individual control points   Highly inexperienced staff performing testing and evaluation   Very little, if at all, integration of annual engagement and ICOFR activities

IT controls need to be streamlined to pertain to true risk of financial exposure. So many areas are far fetched. There are good security principals covered, however they don't pertain to the risks of financial misstatement.

The results from the PCAOB's review seems to be inconsistent with the guidance provided earlier in 2005. Our external audit team focused on some areas that management had determined not to be significant and asked management to re-assess their significant transactions and accounts in November of 2005.

1/ External auditors are getting unfairly enriched by having dual certifications of ICFR.   2/ The scope of the 404 external audit only appears to be limited by their staff availability. During SOX year 2, 60% of the external auditor's staff were college interns who had no audit experience, but nonetheless were billed at full hourly rates.   3/ External auditors appear to only superficially understand internal controls.   4/ Our external auditors claim that they can't share with us their risk assessments and testing scope. Of course not - if they did, we might be able to challenge their scoping decisions and likely lower their fees.

Please take a moment to identify any key §404 topics not addressed in this survey or additional comments you would like to share: (Continued)

The intention of this law was admirable; however, the implementation has resulted (in our case) in an enormous expenditure of money and time without a compensating return. This has hurt rather than helped shareholder value. We could have been spending time on fixing and improving our processes and controls, instead of this truly awful documentation exercise designed to protect our external auditors. This is an example of law of unintended consequences.

Who polices our externals? If they can choose to not share PCAOB reviews, what value does that provide to us? I believe these reviews should be public knowledge! All of our assertions are public.....why don't the externals have to follow the same rules? It's all a money grab until we hold the external firms publicly accountable!!! This is the least they can do to justify their exorbitant fees!!

Financial statement disclosures

The timing and coverage required (testing samples) through the 3Qtr vs. cycle testing is a huge cost driver and should be eliminated.

Please take a moment to identify any key §404 topics not addressed in this survey or additional comments you would like to share: (Continued)

A key issue is PCAOB closed door meetings with the audit firms. Audit firms cite these meetings for their interpretation of the PCAOB guidance and there is not room for discussion after that. This system is now set that the auditor has the only vote in any discussion regarding a reporting matter.

Our external auditor refuses to share with us what they consider to be key controls, so that we can be sure to test/emphasize those controls, especially in areas where management has determined any of those controls not to be key. we believe that this will assist in integrating the testing process, however their view is that to share that information with us impairs their independence. We disagree on this, and it impairs our ability to coordinate our activities.

This survey was very comprehensive. The PCAOB reviews have only commented where too little work was done, not too much. That is one of their weaknesses.

Please take a moment to identify any key §404 topics not addressed in this survey or additional comments you would like to share: (Continued)

SOX 404 appears to have created a conflict of interest in External Audit. There is no impetus to reduce 404 testing or to coordinate efforts with Internal Audit - as this would reduce external audit fees and relinquish some level of independence creating a liability (borne from the purpose of SOX) that External Audit uses for justification of redoing all testwork. Also, the layering of fiduciary responsibility and oversight is redundant. Does the overall cost of SOX offset the material deficiencies that would otherwise have gone undetected? Would SOX have caught the breach at Enron? What is the purpose of lead workers, supervisors, managers, and directors - and can some of that layering be replaced by the review processes now performed by Internal and External Audit as a result of SOX? I think not - but perhaps the better cost would not be spent on 404 testing but on Fraud forensics.

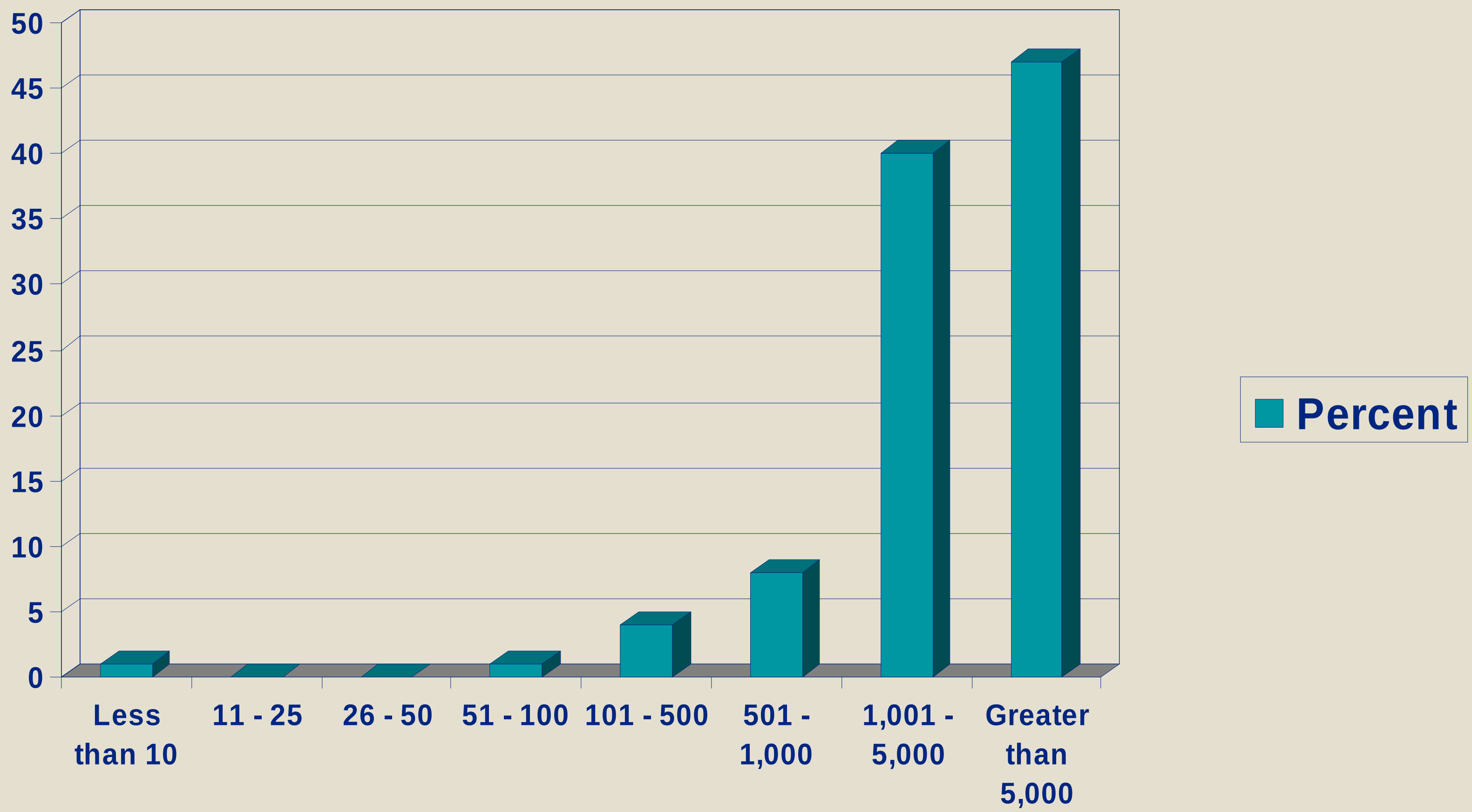
What industry best represents your industry?

Choice	Count	Percentage of Sample Answering	Percentage of Sample Asked	Percentage of Total Sample
Agriculture / Forestry / Fisheries	0	0.0%	0.0%	0.0%
Communication / Telecommunication Services	10	9.6%	7.6%	7.6%
Construction	0	0.0%	0.0%	0.0%
Consulting Services	2	1.9%	1.5%	1.5%
Educational Services	0	0.0%	0.0%	0.0%
Energy	3	2.9%	2.3%	2.3%
Financial Services / Real Estate	8	7.7%	6.1%	6.1%
Gaming / Lotteries	3	2.9%	2.3%	2.3%
Health Services	4	3.8%	3.1%	3.1%
Insurance Carries / Agents	3	2.9%	2.3%	2.3%
Local Government	0	0.0%	0.0%	0.0%
National / Federal Government	0	0.0%	0.0%	0.0%
Manufacturing	25	24.0%	19.1%	19.1%
Technology	8	7.7%	6.1%	6.1%
Transportation	6	5.8%	4.6%	4.6%
Utilities	7	6.7%	5.3%	5.3%
Wholesale / Retail	16	15.4%	12.2%	12.2%
Other; please specify:	9	8.7%	6.9%	6.9%

What other industry best represents your organization?

Temporary staffing
Media Service Provider
Personal service
Industrial distribution
Media/Entertainment
BioTech/Pharma
Hospitality and entertainment
Entertainment
Biotech

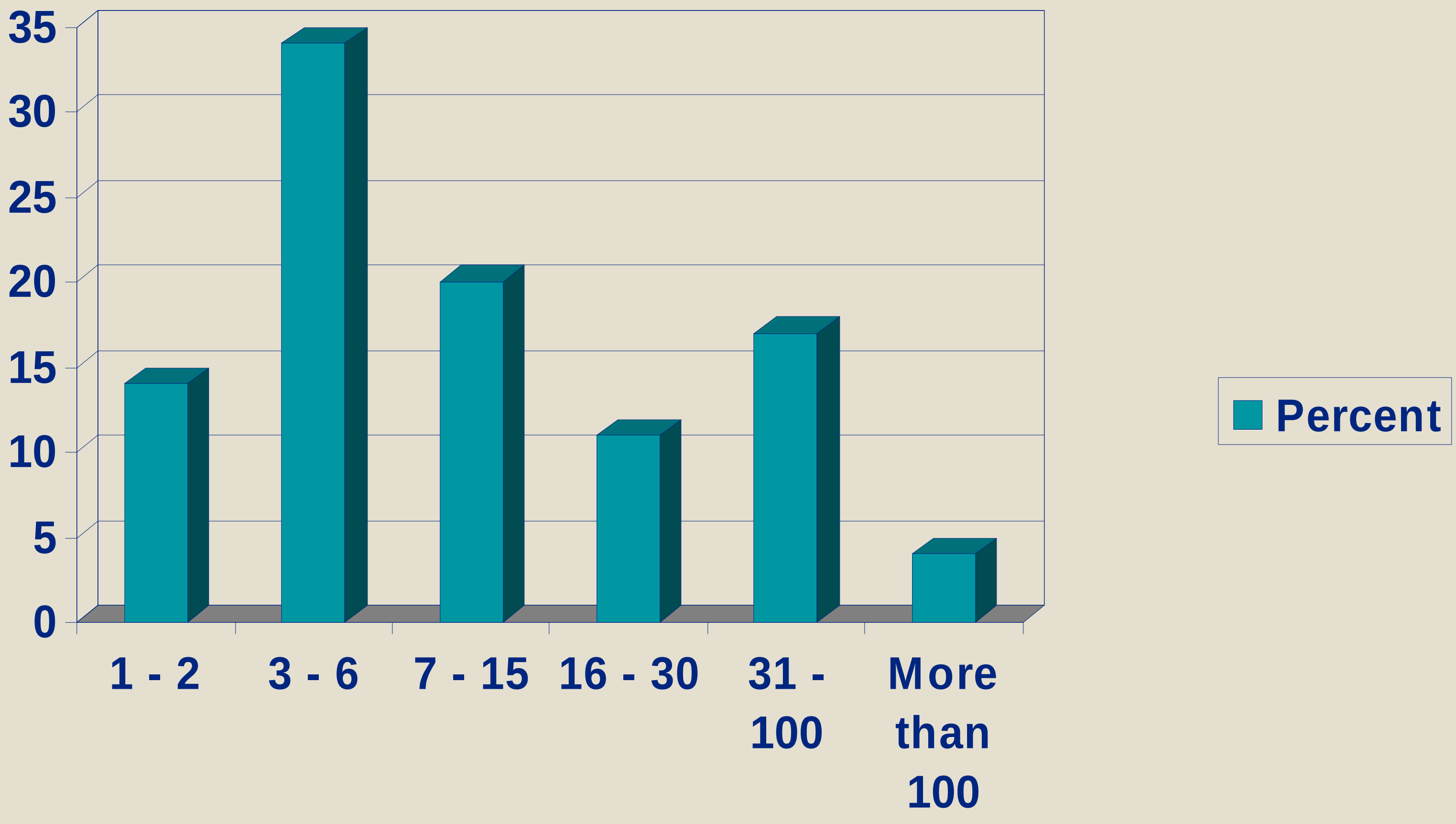
How many full-time equivalents work in your organization?



How many full-time equivalents work in your organization?

Choice	Count	Percentage of Sample Answering	Percentage of Sample Asked	Percentage of Total Sample
Less than 10	1	1.0%	0.8%	0.8%
11 - 25	0	0.0%	0.0%	0.0%
26 - 50	0	0.0%	0.0%	0.0%
51 - 100	1	1.0%	0.8%	0.8%
101 - 500	4	3.8%	3.1%	3.1%
501 - 1,000	8	7.6%	6.1%	6.1%
1,001 - 5,000	42	40.0%	32.1%	32.1%
Greater than 5,000	49	46.7%	37.4%	37.4%

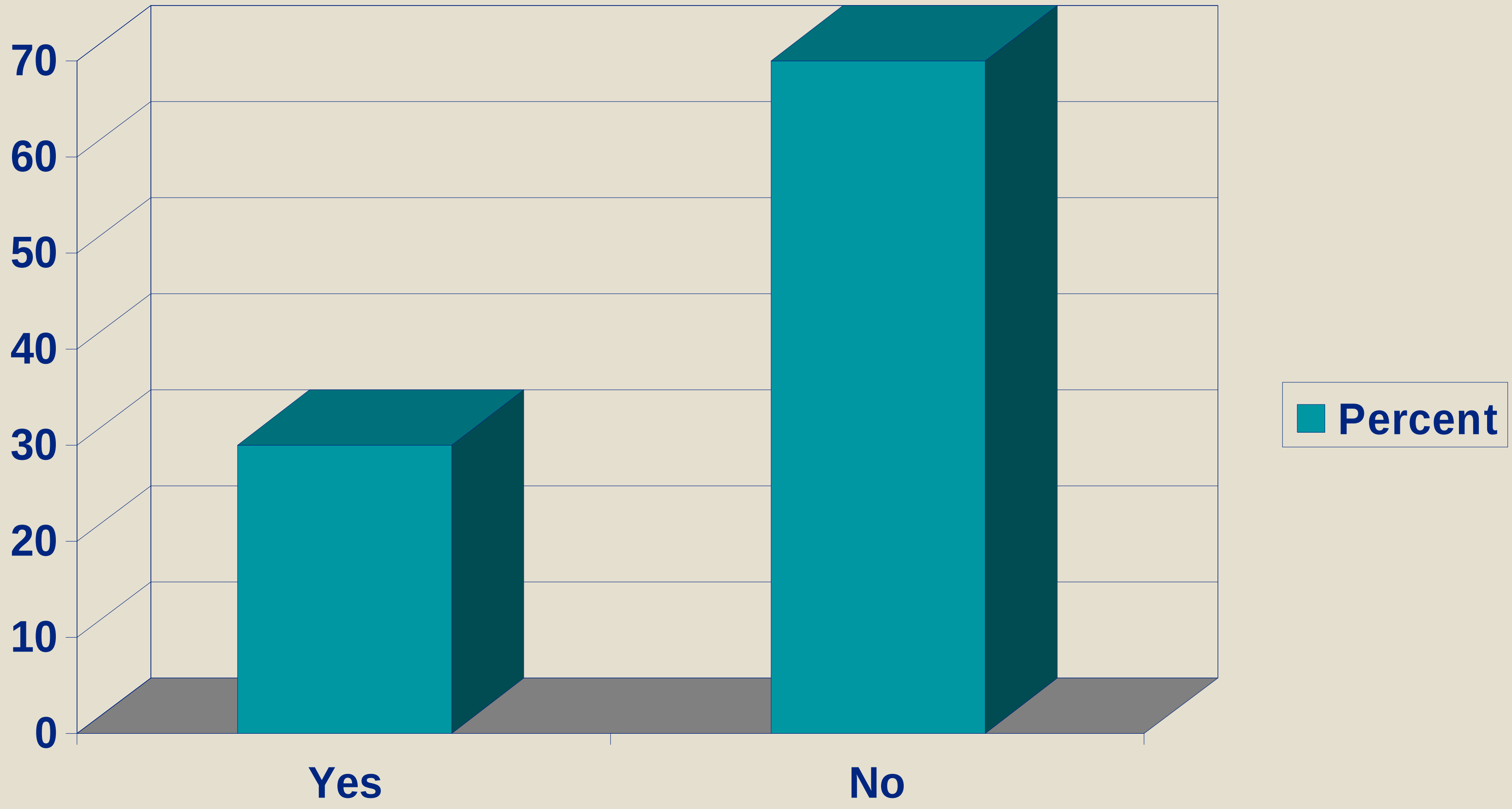
How may full-time equivalents work in your internal audit department?



How may full-time equivalents work in your internal audit department?

Choice	Count	Percentage of Sample Answering	Percentage of Sample Asked	Percentage of Total Sample
1 - 2	15	14.4%	11.5%	11.5%
3 - 6	35	33.7%	26.7%	26.7%
7 - 15	21	20.2%	16.0%	16.0%
16 - 30	11	10.6%	8.4%	8.4%
31 - 100	18	17.3%	13.7%	13.7%
More than 100	4	3.8%	3.1%	3.1%

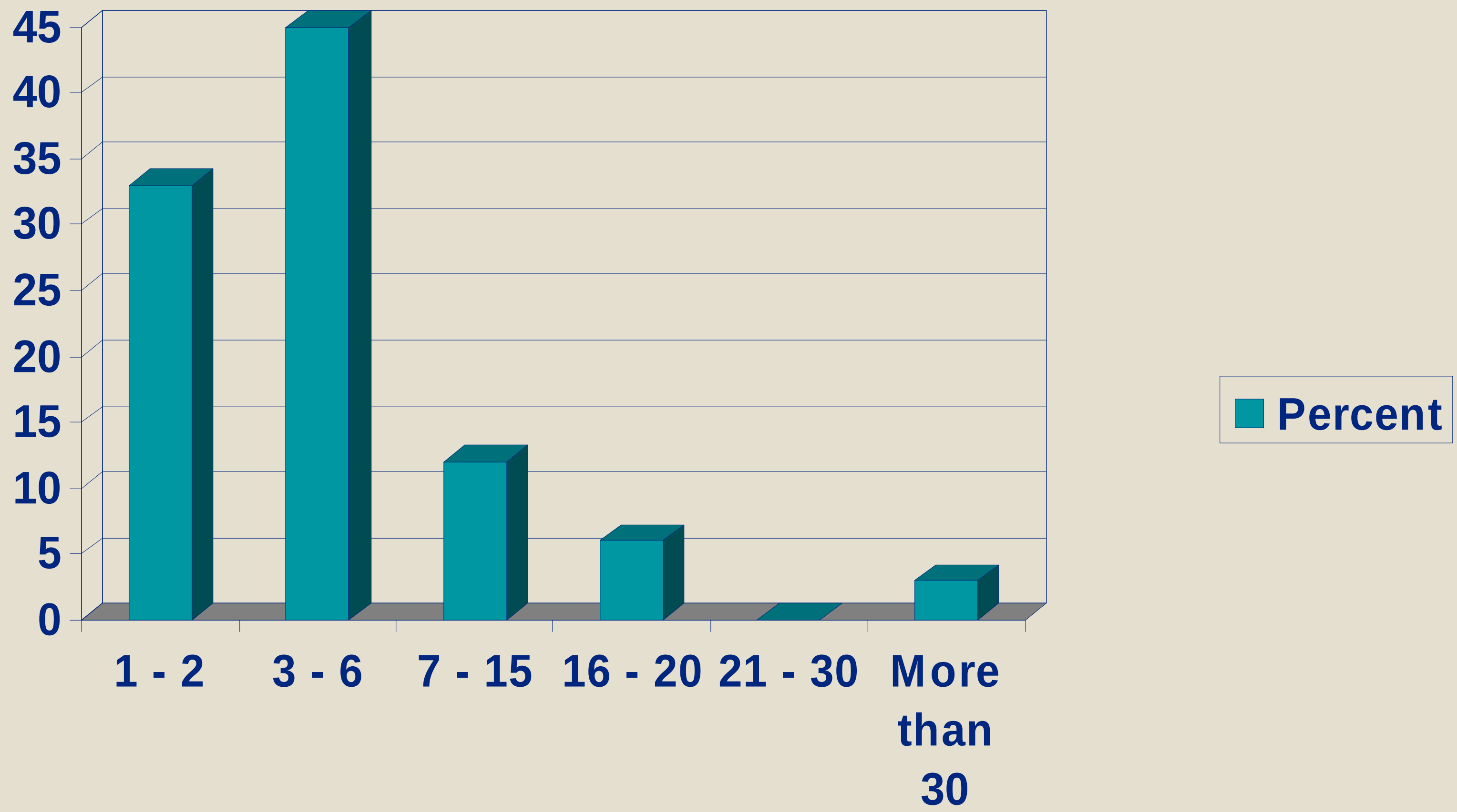
Has your organization created a function separate from internal audit to address Sarbanes-Oxley, specifically §404 work?



Has your organization created a function separate from internal audit to address Sarbanes-Oxley, specifically §404 work?

Choice	Count	Percentage of Sample Answering	Percentage of Sample Asked	Percentage of Total Sample
Yes	32	30.5%	24.4%	24.4%
No	73	69.5%	55.7%	55.7%

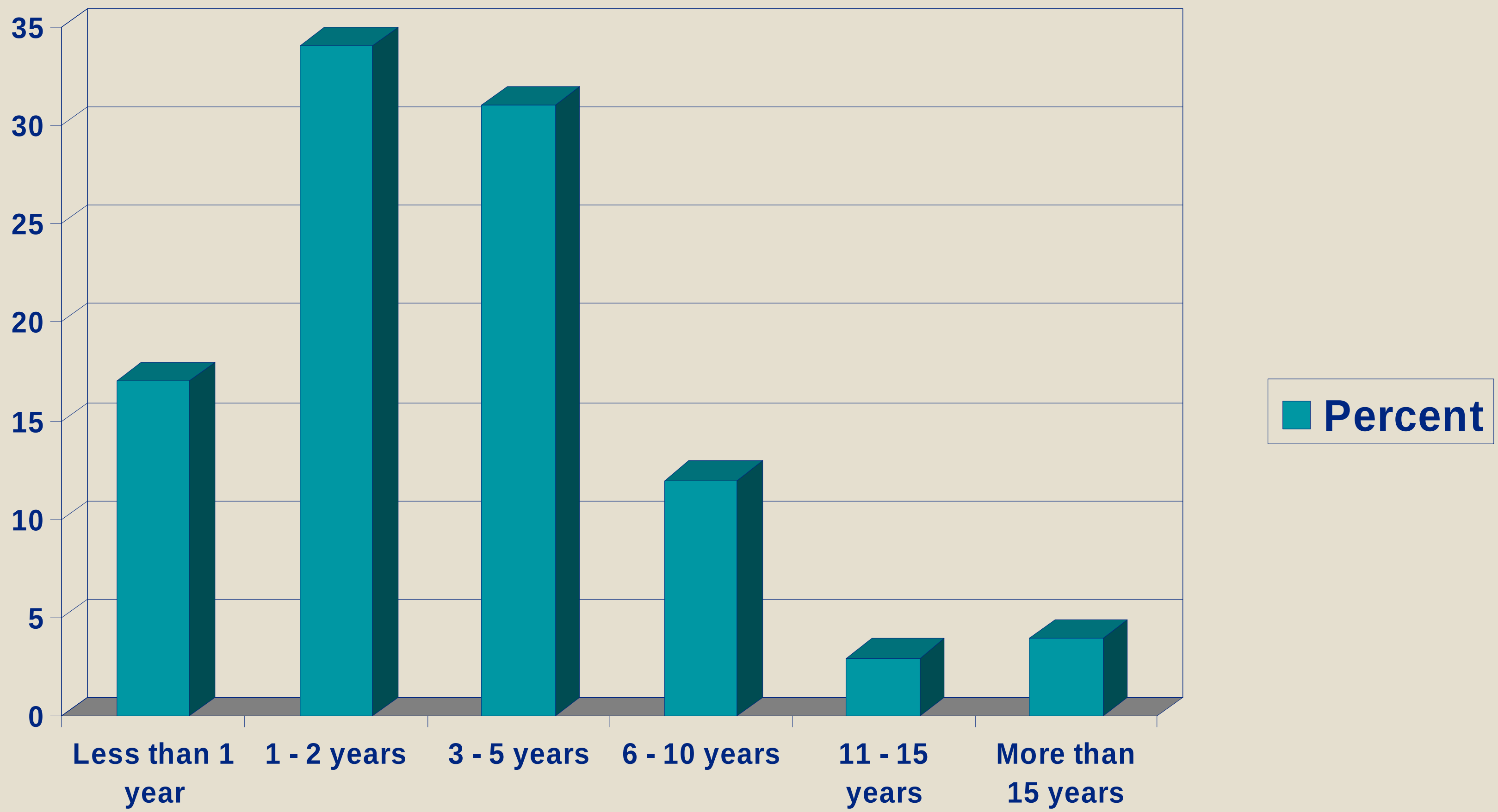
If you have a separate function specific to §404 work, how many full-time equivalents work in this function?



If you have a separate function specific to §404 work, how many full-time equivalents work in this function?

Choice	Count	Percentage of Sample Answering	Percentage of Sample Asked	Percentage of Total Sample
1 - 2	11	33.3%	8.4%	8.4%
3 - 6	15	45.5%	11.5%	11.5%
7 - 15	4	12.1%	3.1%	3.1%
16 - 20	2	6.1%	1.5%	1.5%
21 - 30	0	0.0%	0.0%	0.0%
More than 30	1	3.0%	0.8%	0.8%

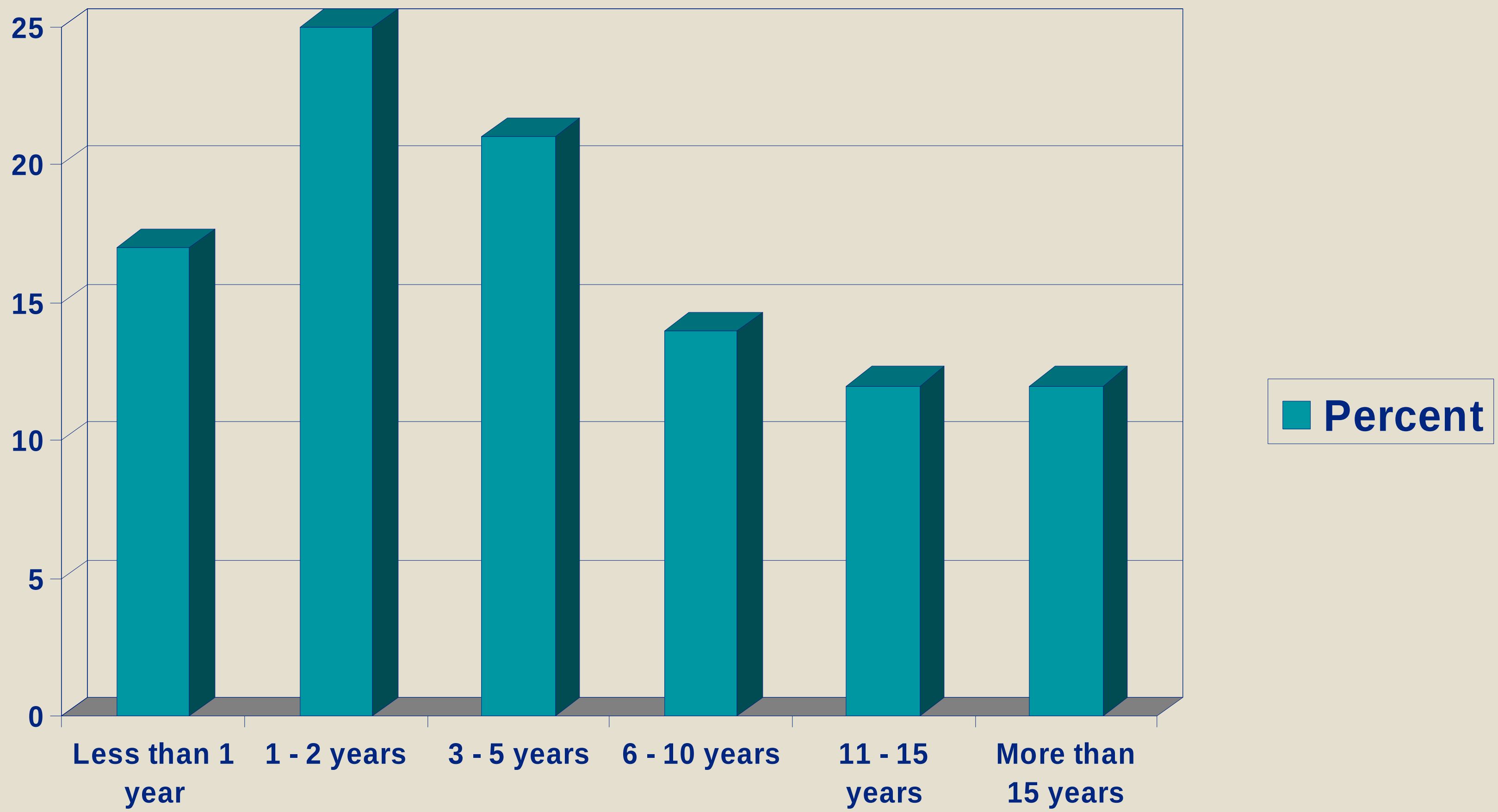
How long have you been in your current position?



How long have you been in your current position?

Choice	Count	Percentage of Sample Answering	Percentage of Sample Asked	Percentage of Total Sample
Less than 1 year	18	17.3%	13.7%	13.7%
1 - 2 years	35	33.7%	26.7%	26.7%
3 - 5 years	32	30.8%	24.4%	24.4%
6 - 10 years	12	11.5%	9.2%	9.2%
11 - 15 years	3	2.9%	2.3%	2.3%
More than 15 years	4	3.8%	3.1%	3.1%

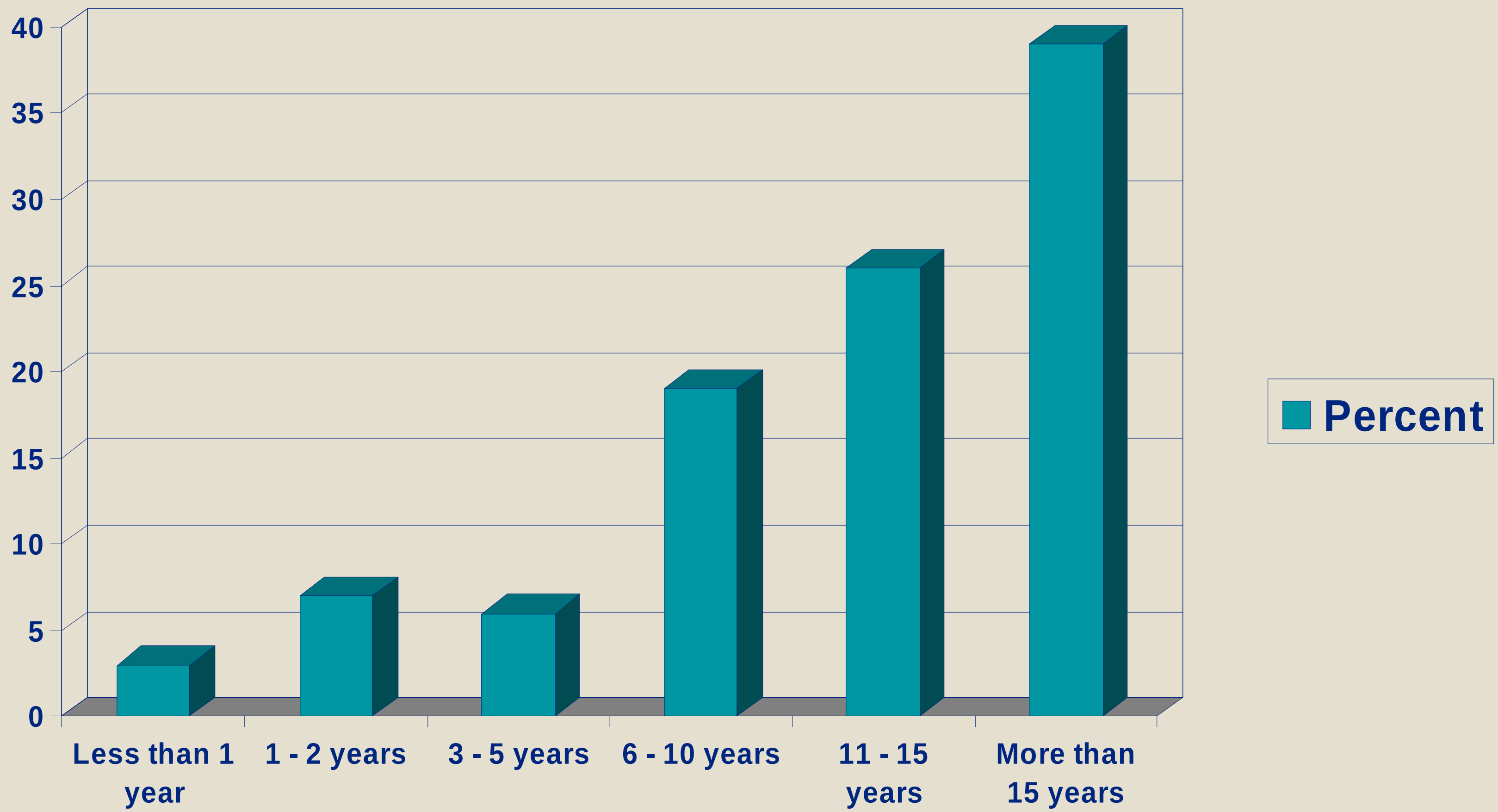
How long have you been with your current organization?



How long have you been with your current organization?

Choice	Count	Percentage of Sample Answering	Percentage of Sample Asked	Percentage of Total Sample
Less than 1 year	17	16.5%	13.0%	13.0%
1 - 2 years	26	25.2%	19.8%	19.8%
3 - 5 years	22	21.4%	16.8%	16.8%
6 - 10 years	14	13.6%	10.7%	10.7%
11 - 15 years	12	11.7%	9.2%	9.2%
More than 15 years	12	11.7%	9.2%	9.2%

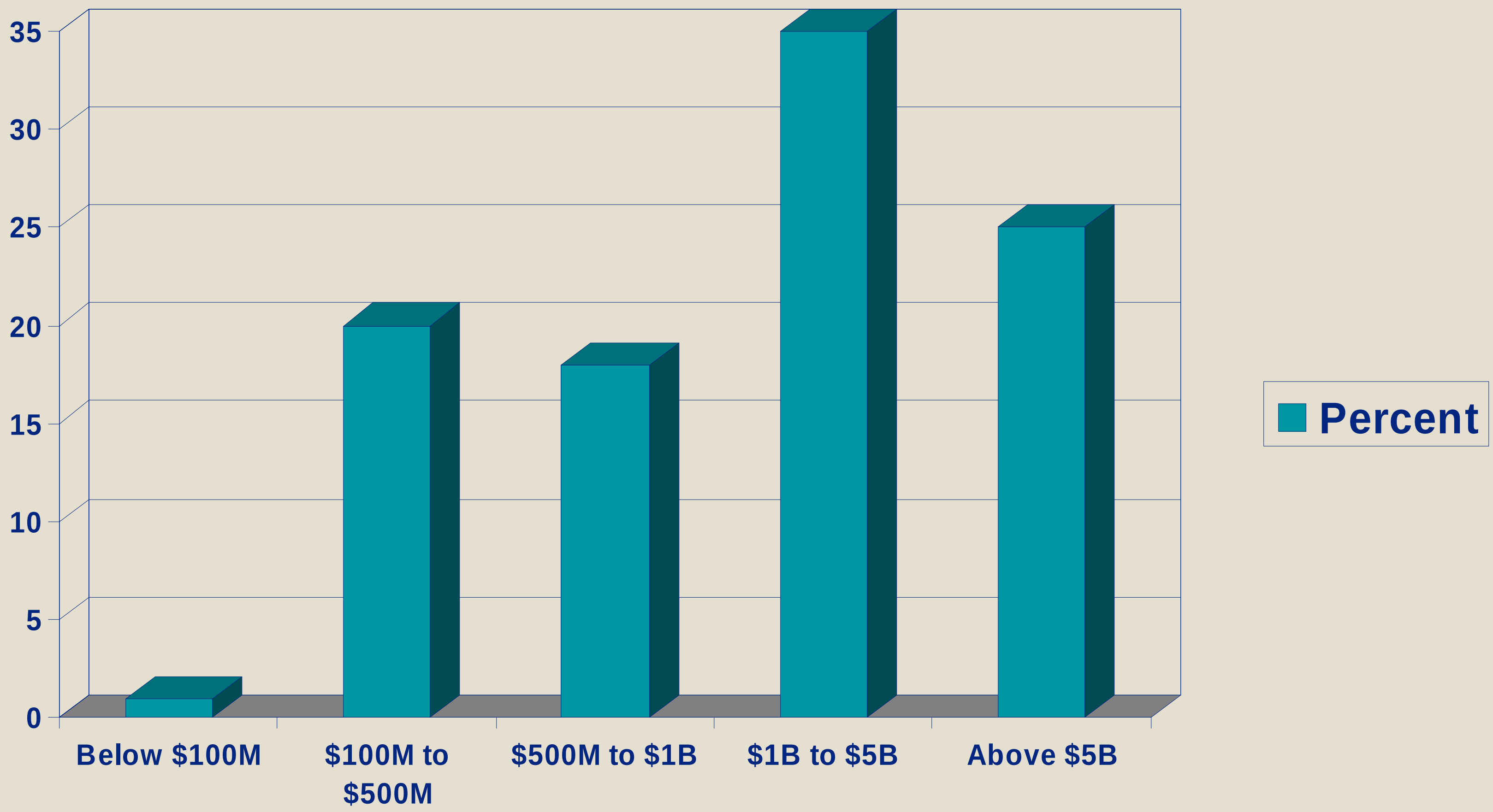
How long have you been in the internal audit profession?



How long have you been in the internal audit profession?

Choice	Count	Percentage of Sample Answering	Percentage of Sample Asked	Percentage of Total Sample
Less than 1 year	3	2.9%	2.3%	2.3%
1 - 2 years	7	6.9%	5.3%	5.3%
3 - 5 years	6	5.9%	4.6%	4.6%
6 - 10 years	19	18.6%	14.5%	14.5%
11 - 15 years	27	26.5%	20.6%	20.6%
More than 15 years	40	39.2%	30.5%	30.5%

What are the annual revenues of your organization?



What are the annual revenues of your organization?

Choice	Count	Percentage of Sample Answering	Percentage of Sample Asked	Percentage of Total Sample
Below $100M	1	1.0%	0.8%	0.8%
$100M to $500M	21	20.4%	16.0%	16.0%
$500M to $1B	19	18.4%	14.5%	14.5%
$1B to $5B	36	35.0%	27.5%	27.5%
Above $5B	26	25.2%	19.8%	19.8%

SARBANES-OXLEY SECTION 404:

A Guide for Management by Internal Controls Practitioners

The Institute of Internal Auditors

PROFESSIONAL GUIDANCE
Setting the Standard

This is the first publication in the Professional Guidance series of the Professional Practices Framework.

The series sets out to tackle subjects of global importance to a wide constituency of IIA members and others. The material includes matters of internal audit principle or practice, and issues of a broader social importance on where The Institute should be able to make a valuable contribution.

Sarbanes-Oxley Section 404: A Guide for Management by Internal Control Practitioners is the product of The Institute of Internal Auditors (the recognized authority and standard-maker in internal auditing in the United States and around the world) and is written for management by those who have worked on internal controls hand-in-hand with board and management — experienced internal auditors.

This ***Guide*** incorporates and reflects up-to-date guidance from the U.S. Securities and Exchange Commission (SEC), the Public Company Accounting Oversight Board (PCAOB), The Institute of Internal Auditors (IIA), and the real-world experience and insight of practicing internal auditors. As management, regulators, and internal and external auditors increase their understanding of the practical aspects of Section 404, and as related rules, regulations, and guidance change, this guide will be updated electronically to reflect new guidance and best practices. To keep updated, please visit ***www.theiia.org***.

Cost is an issue for all management teams. This guide focuses on how total costs can be minimized without impairing the effectiveness of the program.

The guide also discusses the interplay between the requirements of Section 404 and those of Section 302. The latter requires annual and quarterly certifications by the chief executive officer (CEO) and chief financial officer (CFO)[ii] that include assessments of internal controls.

We encourage you to review your plans for Section 404 with the head of your internal audit function, especially how you will ensure that your ongoing program for the years to come is efficient and minimizes disruption to the business. The internal auditor is uniquely positioned not only to review and test your controls, but also to provide internal consulting on the adequacy of their design and on the whole management assessment and testing process. This guide contains a checklist that will be of value in assessing the efficiency of your program.

About The IIA *- Established in 1941, The IIA has more than 115,000 members worldwide. It serves as the internal audit profession's global voice, recognized authority, acknowledged leader, principal educator, and chief advocate. The Institute monitors legislation, regulations and pronouncements of other professional organizations throughout the world on matters that directly impact the practice of internal auditing. It promulgates the* International Standards for the Professional Practice of Internal Auditing *and offers a variety of leading-edge professional development opportunities, a comprehensive certification program, thorough quality assessment services, benchmarking surveys, and valuable research reports and educational products through The IIA Research Foundation. For more information, please visit www.theiia.org.*

TABLE OF CONTENTS

Organizations that have not completed their first year's Section 404 program (non accelerated filers and foreign registrants) can use this guide to ensure their program is not only effective but cost-effective.

On the other hand, organizations that have completed an assessment can use this guide to:

- Assess the efficiency of their Section 404 program, including how to minimize total cost (including external auditor fees).
- Revisit their assessment process and compare it to best practices identified by experienced internal control practitioners.
- Reconsider their processes for assessing deficiencies and providing an overall opinion. Management should provide an opinion that is based on principles instead of rules — in other words, an opinion that provides the investor with a fair assessment of the system of internal control. It should reflect the true condition of the internal control system, not one that is based on technicalities and could mislead the investor, who needs to have confidence in the financial reports.

Based on their role within the organization and their responsibilities for Section 404, readers may use the guide in its entirety or read selectively based on interest.

The first and last sections — "Summary for the CEO and CFO" and "Closing Thoughts on Efficiency" — merit all readers' review.

INTRODUCTION

Much has been written on the subject of Section 404 of the U.S. Sarbanes-Oxley Act of 2002 and management's annual assessment of its system of internal control over financial reporting. Each of the major accounting firms (as well as other providers of audit services) has given us extensive and valuable guidance,[i] generally consistent with the PCAOB's Auditing Standard No. 2 (AS 2), "An Audit of Internal Control Over Financial Reporting Performed in Conjunction With an Audit of Financial Statements" and related Frequently Asked Questions (FAQ).

Management actions are governed by the SEC and not the PCAOB. In practice, the SEC has endorsed the principles in AS 2, which it formally approved for publication in June 2004. However, it is not written as a guide for management, but rather as a standard for the external auditor. The various publications of the accounting firms, while valuable and necessary reading, are influenced by their perspectives.

Internal auditors specialize in the assessment of internal controls and have for decades. They do so as a service to the audit committee and management of their organizations and, therefore, have extensive insight into the operation of those controls and the constraints on management in providing those controls. They are experts in the theory and practice of internal controls and related auditing.

The costs and benefits of the U.S. Sarbanes-Oxley Act of 2002 have both received a lot of ink as organizations prepared for and issued their first assessments of internal control over financial reporting as required by Section 404. In truth, there have been a lot of complaints by executives over the tremendous additional costs and the discussion of benefits has been muted in comparison.

When U.S. Congress passed the Act, the intent was to drive improvements in companies' internal controls. The benefits were seen as greater assurance to shareholders and other stakeholders in published financial reports; costs were of lesser significance. However, cost is of tremendous importance to corporate executives.

In November 2005, the PCAOB issued a report[iii] that commented on efficiencies, both in management's and the external auditors' work:

> "The Board's monitoring has focused on whether firms' audit methodologies, as well as firms' execution of those methodologies, have resulted in audits of internal control that are effective and efficient. The Board found that both firms and issuers faced enormous challenges in the first year of implementation, arising from the limited time frame that issuers and auditors had to implement Section 404; a shortage of staff with prior training and experience in designing, evaluating, and testing controls; and related strains on available resources. These challenges were compounded in those companies that needed to make significant improvements in their internal control systems to make up for deferred maintenance of those systems.

> "The Board's monitoring revealed that audits performed under these difficult circumstances were often not as effective or efficient as Auditing Standard No. 2 intends (and as the Board expects they can be in the future, given the benefits of experience, adequate time, and resources)."

KEY POINTS

PCAOB FINDINGS

"Both firms and issuers faced enormous challenges in the first year of implementation, arising from the limited time frame that issuers and auditors had to implement Section 404; a shortage of staff with prior training and experience in designing, evaluating, and testing controls; and related strains on available resources."

"Audits performed under these difficult circumstances were often not as effective or efficient as Auditing Standard No. 2 intends."

This guide, which is focused on achieving success at the lowest possible total cost, including external auditor fees, can help management tasked with responsibility for the Section 404 program by providing:

- Information on the requirements of Sarbanes-Oxley and the fundamentals of internal controls.
- A discussion of how the annual requirements of Section 404 relate to the quarterly requirements of Section 302 (the quarterly certification by the CEO and CFO).
- An explanation and practical suggestions for each phase of the program, including areas of difficulty: identification of key controls, assessing deficiencies, and the final assessment.

- Advice on how to reach a fair assessment that does not mislead investors as to the condition of internal controls and the reliability of financial statements. Even though many companies (and their external auditors) have taken a rules-based approach, management needs to ensure their assessment is principles-based. Management's formal assessment has to reflect their belief as to whether the controls provide reasonable assurance of the reliability of *future*[1] financial statements.[iv] That reliability is based on the likelihood of an error that would be material to a reasonable investor. An assessment that the controls are not effective simply because there has been a restatement may mislead the investor as to the *current* state of internal controls and the reliability of future financial statements.
- A checklist to help management assess the efficiency of their program.

Some companies have adopted a methodology for Section 404 that is rules-based.[v] This can lead to an assessment that is neither effective nor efficient. Instead, management should use judgment to develop and operate a continuing Section 404 program that is principles-based. Executives should understand that:

- The SEC, which is the governing authority for corporations, has only provided general guidance and very few specific rules. However, it has approved the standards developed by the PCAOB — the rule-maker for the external audit firms.
- Management has a great deal of flexibility in designing and implementing their Section 404 program, much more than is available to the external auditor.
- Both management and the external auditor have been encouraged by the SEC and the PCAOB to use their judgment and develop an approach that is top-down and risk-based.The Section 404 program should include coverage of all areas where the inherent risk (i.e., the risk before the quality of internal controls is considered) of an error that could lead to a material misstatement[vi] is at least reasonably possible[vii]. There is no need for the program to assess and test every control related to financial reporting, even those that might be considered significant deficiencies if they failed (see the definition of significant deficiency provided later in this guide).

> ***KEY POINTS***
>
> **MANAGEMENT'S ROLE**
>
> *Management has a great deal of flexibility in designing and implementing their Section 404 program, much more than is available to the external auditor.*
>
> *Both management and the external auditor have been encouraged by the SEC and the PCAOB to use their judgment and develop an approach that is top-down and risk-based.*

---

[1]The guidance published by the SEC and PCAOB does not address this issue directly. However, there are indications in comments by officials with these organizations that the value of the Section 404 assessment is that it provides a level of comfort with respect to the reliability of future financial statements (on the assumption that there is no significant change in the quality of the system of internal control). The quality of the system of internal control at the end of the reporting year is an indication of whether it is sufficiently robust to either prevent or detect material misstatements in financial statements that will be prepared under the processes and related controls that management has assessed. In addition, an assessment of the likelihood of any event is difficult, if not impossible, without defining the period during which the event may occur. In this guide, the authors have taken the reasonable position that management's assessment should reflect the likelihood of a material misstatement in one or more of the next 12 months' financial statement filings. Neither the SEC nor the PCAOB have publicly commented on this matter, and our position relative to 12 months (which would include the next annual financials on Form 10-K as well as interim reports on Form 10-Q) is a suggestion based on what we believe is reasonable.

On May 16, 2005, the SEC staff issued a "Statement on Management's Report on Internal Control over Financial Reporting" that said (emphasis added):

> "An overall purpose of internal control over financial reporting is to foster the preparation of reliable financial statements. Reliable financial statements must be materially accurate. Therefore, a central purpose of the assessment of internal control over financial reporting is to identify material weaknesses that have, as indicated by their very definition, more than a remote likelihood of leading to a material misstatement in the financial statements. While identifying control deficiencies and significant deficiencies represents an important component of management's assessment, *the overall focus of internal control reporting should be on those items that could result in material errors in the financial statements.*
>
> "In adopting its rules implementing Section 404, the Commission expressly declined to prescribe the scope of assessment or the amount of testing and documentation required by management. *The scope and process of the assessment should be reasonable, and the assessment (including testing) should be supported by a reasonable level of evidential matter. Each company should also use informed judgment in documenting and testing its controls to fit its own operations, risks and procedures. Management should use its own experience and informed judgment in designing an assessment process that fits the needs of that company. Management should not allow the goal and purpose of the internal control over financial reporting provisions — the production of reliable financial statements — to be overshadowed by the process."*

KEY POINTS

SEC STAFF STATEMENT

"While identifying control deficiencies and significant deficiencies represents an important component of management's assessment, the overall focus of internal control reporting should be on those items that could result in material errors in the financial statements."

"Each company should also use informed judgment in documenting and testing its controls to fit its own operations, risks and procedures. Management should use its own experience and informed judgment in designing an assessment process that fits the needs of that company. Management should not allow the goal and purpose of the internal control over financial reporting provisions — the production of reliable financial statements — to be overshadowed by the process."

Similarly, the PCAOB's May 16, 2005, Policy Statement noted (the emphasis is from the Policy Statement):

"… to properly plan and perform an effective audit under Auditing Standard No. 2, auditors should:

- ***exercise judgment to tailor their audit plans to the risks facing individual audit clients,*** instead of using standardized "checklists" that may not reflect an allocation of audit work weighted toward high-risk areas (and weighted against unnecessary audit focus in low-risk areas);
- ***use a top-down approach*** that begins with company-level controls, to identify for further testing only those accounts and processes that are, in fact, relevant to internal control over financial reporting; and

- ***use the risk assessment required by the standard*** to eliminate from further consideration those accounts that have only a remote likelihood of containing a material misstatement."

Executives should also understand that:

- Management is *not* required to adopt the same methodology as the external auditor, although there may be advantages in using a similar approach. The PCAOB's AS 2 is mandatory for external auditors, not for management.
- The rules-based approach favored by some external auditors may tend toward an assessment of the overall system of controls that is not a fair representation, in the judgment of management, of their condition.

> *KEY POINT*
>
> **SEC 404 ASSESSMENT**
>
> *The Section 404 assessment indicates to the investor whether the system of internal control is sufficiently robust such that the risk of material error in future financial statements is remote or less.*

- The regulators believed the greatest benefit from Section 404 was that it would provide greater assurance to investors and others that they could rely on management's published financials. The value of that assurance is not as it relates to the current set of financial statements (to which the Section 404 assessment is attached), as they are subject to a separate assertion by management and opinion by the external auditor on their adequacy. Neither is the value in assessing controls over prior period financials. The value is in providing comfort with respect to the reliability of financial statements that will be published in the *future*. The Section 404 assessment indicates to the investor whether the system of internal control is sufficiently robust such that the risk of material error in *future* financial statements is remote or less[viii].

In practical terms, management's assessment of the system of internal control over financial reporting should reflect whether they believe the risk of material misstatements in financial statements filed with the SEC during the next 12 months[2] is less than reasonably likely. An alternative view is whether management believes its system of internal control over financial reporting contains any material weaknesses, representing a more than remote risk that financial statements filed with the SEC during the next 12 months will contain material errors.

The greatest area of potential cost-savings is through reduction of external costs (i.e., costs other than internal employees' time).[ix] Many companies continue to make significant use of third-party providers of consulting and audit services to perform testing and sometimes manage their Section 404 program. They are working to reduce these costs by hiring project management and testing personnel.

External auditor fees related to their Section 404 work make up a large part of total costs.[x] In addition to the efficiencies they are making from experience and in response to PCAOB guidelines and recommendations, management can effect fee reductions by:

- Limiting the number of key controls — the controls that have to be tested — by adopting a top-down, risk-based approach that focuses on controls that will prevent or detect material errors. Companies and external auditors have, as confirmed in the PCAOB November

---

[2]*See the earlier footnote(1). The authors recommend using a period of 12 months; however, the SEC and PCAOB have not publicly commented on whether this is an appropriate method.*

2005 report, tested controls that are not key (i.e. - not required to prevent or detect material errors). Controls that are not likely to result in material error should they fail should not be considered "key" and do not need to be within management's scope for Section 404.

- Maximizing reliance by the external auditor on management testing. This requires ensuring management testing is performed by skilled, experienced individuals who are independent of the activity being tested. The latter usually have several years' experience in a combination of external audit firms and internal audit functions. Most companies use their internal audit function to perform the testing; this is the most likely approach to maximize external auditor reliance. Some use other internal staff to perform management testing and rely on internal auditing to review and test their work to ensure it is to appropriate standards.[xi]

KEY POINT

KEY CONTROLS

Controls that are not likely to result in material error should they fail should not be considered "key" and do not need to be within management's scope for Section 404.

- Executing controls flawlessly. The tolerance level for defects in testing is very low. If the external auditors find even one error in their testing of a control, they may assess the control as not operating effectively. This will require remediation and retesting, potentially doubling the work.
- Documenting the processes and controls clearly and in good detail, and then ensuring the documentation is updated promptly as processes change.
- Completing a substantial portion of management's work, including testing (even if only limited in sample size) of all key controls, by mid-year. This enables the external auditors to start their work early, which helps with resource scheduling and reduces the risk of finding deficiencies late.

The above actions will also reduce internal costs, including management and employees' time. The most significant factors are:

- Reduction in the number of key controls.[xii]
- Executing controls flawlessly.

In the past, most CEOs and CFOs have signed their annual and quarterly certifications — which are included in the financial statements filed with the SEC on Form 10-Q, and are required by Section 302 of Sarbanes-Oxley — without a rigorous examination of internal controls. Now that Section 404 is in force (at least for accelerated filers), management should be integrating its quarterly and annual assessment processes. Although management is not required to test all their key controls every quarter, they should perform some degree of testing each quarter to support the quarterly Section 302 certification.[xiii] At minimum, the Section 302 certification process should include a consideration of the status of the Section 404 project, the results of testing, and the severity of any identified control deficiencies.

Companies, external audit firms, and the regulators are all learning how Section 404 should be applied and how both management and the external auditors can be both effective and efficient. The last section of this guide includes a number of questions management may use to assess their programs.

SUMMARY FOR THE CEO AND CFO

The SEC and PCAOB are likely to provide additional guidance. The authors plan to update this guide and provide additional information through other publications to reflect changes in regulations as well as in best practice.

Section 404 of Sarbanes-Oxley required the SEC to develop and publish rules for a management assessment of internal control over financial reporting (ICFR). Those rules were completed in June 2003, and the PCAOB followed with its AS 2, which was approved by the SEC in June 2004. Together, they require that:

- Management perform a formal assessment of its controls over financial reporting (see definition below), including testing to confirm both the design and operating effectiveness of the controls.
- Management include in its annual report on Form 10-K[xiv] an assessment of internal control over financial reporting.
- The external auditors provide three opinions as part of a single integrated audit of the company, instead of the one previously provided. This includes:
  - An opinion on management's assessment.
  - An independent opinion on the effectiveness of the system of internal control over financial reporting.
  - The traditional opinion on the financial statements.

The SEC rules are worth reviewing carefully. They "require a company's annual report to include an internal control report of management that contains:

- A statement of management's responsibility for establishing and maintaining adequate internal control over financial reporting for the company.
- A statement identifying the framework used by management to conduct the required evaluation of the effectiveness of the company's internal control over financial reporting.
- Management's assessment of the effectiveness of the company's internal control over financial reporting as of the end of the company's most recent fiscal year, including a statement as to whether or not the company's internal control over financial reporting is effective. The assessment must include disclosure of any "material weaknesses" in the company's internal control over financial reporting identified by management. Management is not permitted to conclude that the company's internal control over financial reporting is effective if there are one or more material weaknesses in the company's internal control over financial reporting.
- A statement that the registered public accounting firm that audited the financial statements included in the annual report has issued an attestation report on management's assessment of the registrant's internal control over financial reporting."

The "final rules also require a company to file, as part of the company's annual report, the attestation report of the registered public accounting firm that audited the company's financial statements."

Taking each point in turn:

1. Management is responsible for the system of internal control. This is an important clarification, as previously some management teams believed[xv] the system of internal control was the responsibility of internal audit, external audit, or the CFO. By contrast, an effective system of internal control is the responsibility not just of the CFO, but the CEO and the senior executive team as a whole.

2. The assessment has to be made using a recognized internal control framework. Most U.S. companies have used The Committee of Sponsoring Organizations of the Treadway Commission (COSO) framework, although some have used the Control Objectives for Information and related Technology (CobiT) framework as a supplement to COSO for IT controls. Both COSO and CobiT are discussed in Section B of this guide.

3. The assessment is annual and "as of" year-end. There are restrictions on how management can make its assessment, depending on whether a "material" weakness is identified.

4. The external auditor must perform specified work in relation to management's assessment. The SEC mandated "an attestation report." The PCAOB has interpreted that in AS 2, with SEC consent, to include not only an assessment and related formal opinion on management's assessment, but also an independent assessment and formal opinion on the adequacy of the system of internal control over financial reporting.

Although the PCAOB has provided quite detailed (and generally principles-based) guidance for external auditors in AS 2, AS 2 is not binding on management. In fact, management has a great deal of flexibility in implementing its Section 404 program. The guidance from the SEC is principles-based, only requiring an assessment that is based on one of the recognized internal control frameworks.

Management needs to understand AS 2, because it explains how the external auditor will review and assess management's assessment process. It is also important if, to contain cost, management is planning to minimize audit fees by maximizing reliance on management testing.

However, management also needs to ensure its process is faithful to the principles behind Section 404: that it provides a fair assessment of the organization's internal controls as of year-end, reflecting whether the system provides reasonable assurance that material misstatements will be prevented or detected.

The following sections provide a road map for understanding the principles and requirements for Section 404 and implementing an efficient and effective Section 404 program. Section D (page 20) explains the requirements of Section 302 (the quarterly certification by the CEO and CFO of the interim financials) and its relationship with Section 404.

B. REVISITING THE PRINCIPLES OF INTERNAL CONTROL

There are a variety of definitions of *internal control*. For the purposes of Section 404, the great majority of companies and all the Certified Public Accounting (CPA) firms[xvi] use the definition in COSO's *Internal Control – Integrated Framework*. COSO's definition relates to all aspects of internal control, not just that over financial reporting. The following is from the Executive Summary of the COSO report.

> "Internal control is broadly defined as a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:
> - Effectiveness and efficiency of operations.
> - Reliability of financial reporting.
> - Compliance with applicable laws and regulations.
>
> "The first category addresses an entity's basic business objectives, including performance and profitability goals and safeguarding of resources. The second relates to the preparation of reliable published financial statements, including interim and condensed financial statements and selected financial data derived from such statements, such as earnings releases, reported publicly. The third deals with complying with those laws and regulations to which the entity is subject. These distinct but overlapping categories address different needs and allow a directed focus to meet the separate needs."

KEY POINTS

COSO PRINCIPLES OF INTERNAL CONTROL

"Internal control is broadly defined as a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives."

"While internal control is a process, its effectiveness is a state or condition of the process at one or more points in time."

COSO goes on to say:

> "Internal control systems operate at different levels of effectiveness. Internal control can be judged effective in each of the three categories, respectively, if the board of directors and management have reasonable assurance that:
> - They understand the extent to which the entity's operations objectives are being achieved.
> - Published financial statements are being prepared reliably.
> - Applicable laws and regulations are being complied with.
>
> "While internal control is a process, its effectiveness is a state or condition of the process at one or more points in time."

The PCAOB, together with the SEC, is responsible for the rules governing the roles and actions of the CPA firms. In AS 2, "An Audit of Internal Control Over Financial Reporting Performed in Conjunction With an Audit of Financial Statements," the PCAOB has a definition that is consistent with that of COSO, although limited to financial reporting. It is also consistent in all material respects with the definition used by the SEC.[xvii] They define ICFR as:

> "A process designed by, or under the supervision of, the company's principal executive and principal financial officers, or persons performing similar functions, and effected by the company's board of directors, management, and other personnel, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial

statements for external purposes in accordance with generally accepted accounting principles (GAAP) and includes those policies and procedures that:

- Pertain to the maintenance of records that, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the company;
- Provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the company are being made only in accordance with authorizations of management and directors of the company; and
- Provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the company's assets that could have a material effect on the financial statements."

There are a number of key points in these definitions:

1. Internal control is a *process*. It is a continuing process rather than a point-in-time situation. However, any assessment of its effectiveness is made at a point in time. Management must assess the adequacy of its ICFR as of year-end, even though the system operates continuously - not only all year but for multiple years. Management needs to be aware, though, that an assessment as of a point in time is likely to be interpreted by investors and others as indicative of its continuing effectiveness. Stakeholders are concerned with whether or not the internal controls are sufficient to provide comfort, not only with respect to the reliability of the current set of financial statements, but also of future financial statements.

2. Internal control only provides *reasonable assurance*. The COSO Executive Summary expands on this point:

   "An internal control system, no matter how well conceived and operated, can provide only reasonable — not absolute — assurance to management and the board regarding achievement of an entity's objectives. The likelihood of achievement is affected by limitations inherent in all internal control systems. These include the realities that judgments in decision-making can be faulty, and that breakdowns can occur because of simple error or mistake.

   Additionally, controls can be circumvented by the collusion of two or more people, and management has the ability to override the system. Another limiting factor is that the design of an internal control system must reflect the fact that there are resource constraints, and the benefits of controls must be considered relative to their costs."

KEY POINT

REASONABLE ASSURANCE

"An internal control system, no matter how well conceived and operated, can provide only reasonable — not absolute — assurance to management and the board regarding achievement of an entity's objectives. The likelihood of achievement is affected by limitations inherent in all internal control systems. These include the realities that judgments in decision-making can be faulty, and that breakdowns can occur because of simple error or mistake."

The PCAOB's AS 2 also discusses reasonable assurance, taking it further to establish that *reasonable* is a "high level of assurance":

> "Management's assessment of the effectiveness of internal control over financial reporting is expressed at the level of reasonable assurance. The concept of reasonable assurance is built into the definition of internal control over financial reporting and also is integral to the auditor's opinion. Reasonable assurance includes the understanding that there is a remote likelihood that material misstatements will not be prevented or detected on a timely basis. Although not absolute assurance, reasonable assurance is, nevertheless, a high level of assurance."

An effective system of internal control can only provide this reasonable assurance. When assessing its adequacy, management needs to determine whether errors — even if they resulted in a material error in the financial statements — are the result of a "simple error or mistake" that is a momentary or one-time failure, rather than an indication that the system no longer provides reasonable assurance that a material error in the financials will not be prevented or detected. COSO, PCAOB, and the SEC refer to the concept of a reasonable person's view, which should be considered when assessing whether the system of internal control provides reasonable assurance.

The PCAOB states that *reasonable* is a "high level of assurance." They refer to the "understanding that there is a *remote likelihood* that material misstatements will not be prevented or detected on a timely basis." This is fully consistent with the way in which management and the external auditor should assess the overall system of internal control. As noted later, the external auditors typically use a range of 5 percent to 10 percent for remote likelihood.

The SEC has not provided a specific standard with which the effectiveness of internal control should be measured. Instead, in the words of their commentary on the final rules, they have set a "threshold for concluding that a company's internal control over financial reporting is effective." That threshold is the presence of one or more material weaknesses. Therefore, management can assess ICFR as effective if there are no control deficiencies such that a material error is reasonably possible.

Stating the issue perhaps more simply, a system of internal control provides a reasonable level of assurance with respect to filed financial statements (i.e., for Section 404) when:

- The cumulative risk of a material misstatement due to known control weakness is not reasonably possible, i.e. 10 percent or less.[3]
- Any control weaknesses identified by management and external or internal auditors are corrected promptly.
- The management team believes the level of controls is appropriate to the business, enabling reliable financial reporting for external use (i.e., SEC filings).

[3] *The 10 percent reference is based on the external auditors' general use of a range of 5 percent to 10 percent when determining whether the likelihood of a material error is 'more than remote.' Although it is not generally possible to calculate the probability of an error with any degree of precision, and there is no authoritative guidance in this area, this range is helpful in providing management with a feel for the level of probability being discussed.*

3. Internal control over the integrity of a company's financial statements is part of the overall system of internal control. In practice, there can be significant overlap between controls designed to provide assurance over the financials and those that provide assurance relative to operational effectiveness or compliance. For example, monitoring the cost of units sold is an important control for both financial reporting and for ensuring the efficiency and effectiveness of operations. When assessing control deficiencies to determine the need and value of enhancing controls, management should consider the risk not only to the financial statements, but also to the efficiency of operations or compliance with applicable rules and regulations.

4. Another point of significance is that for Section 404 purposes, ICFR only addresses the controls providing assurance over financial statements filed with the SEC. It does not necessarily address controls over:
   - Other financial statements, including those provided as part of statutory reporting to foreign governments or to financial institutions, as may be required by debt instruments.
   - Financial reporting used in internal management decision-making; for example, monthly management metrics.
   - Other sections of the 10-K such as Management's Discussion and Analysis (MD&A).
   - Earnings releases and proxy statements.

Clearly, management needs to have effective controls over all forms of financial reporting and may consider either extending its own assessment to cover these areas, or asking its internal audit function to perform procedures relative to these areas.

THE COSO FRAMEWORK

Management is required to assess its system of ICFR using a recognized framework. Most have selected the COSO framework, which is recognized as appropriate by both the SEC and the PCAOB.

COSO's internal control framework describes internal controls as consisting of five inter-related components. These are generally called "layers," and the controls within each must be included in management's assessment. The five layers are described by COSO as:

1. **Control Environment**

   "The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Control environment factors include the integrity, ethical values, and competence of the entity's people; management's philosophy and operating style; the way management assigns authority and responsibility, and organizes and develops its people; and the attention and direction provided by the board of directors."

2. **Risk Assessment**

   "Every entity faces a variety of risks from external and internal sources that must be assessed. A precondition to risk assessment is establishment of objectives, linked at different levels and internally consistent. Risk assessment is the identification and analysis of relevant risks to achievement of the objectives, forming a basis for determining how the risks should be managed. Because economic, industry, regulatory, and operating conditions will continue to change, mechanisms are needed to identify and deal with the special risks associated with change."

3. **Control Activities**

   "Control activities are the policies and procedures that help ensure management directives are carried out. They help ensure that necessary actions are taken to address risks to achievement of the entity's objectives. Control activities occur throughout the organization, at all levels and in all functions. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets, and segregation of duties."

4. **Information and Communication**

   "Pertinent information must be identified, captured, and communicated in a form and time frame that enable people to carry out their responsibilities. Information systems produce reports containing operational, financial, and compliance-related information that make it possible to run and control the business. They deal not only with internally generated data, but also information about external events, activities, and conditions necessary to informed business decision-making and external reporting. Effective communication also must occur in a broader sense, flowing down, across, and up the organization. All personnel must receive a clear message from top management that control responsibilities must be taken seriously. They must understand their own role in the internal control system, as well as how individual activities relate to the work of others. They must have a means of communicating significant information upstream. There also needs to be effective communication with external parties, such as customers, suppliers, regulators, and shareholders."

5. **Monitoring**

   "Internal control systems need to be monitored — a process that assesses the quality of the system's performance over time. This is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two. Ongoing monitoring occurs in the course of operations. It includes regular management and supervisory activities, and other actions personnel take in performing their duties. The scope and frequency of separate evaluations will depend primarily on an assessment of risks and the effectiveness of ongoing monitoring procedures. Internal control deficiencies should be reported upstream, with serious matters reported to top management and the board."

In practice, the assessment of ICFR is conducted at only two levels instead of five. Most of the controls that are assessed are those found in the Control Activities layer. Controls within the other four are typically grouped together; a common term for this group is *entity-level controls*. While the majority of controls are in Control Activities, particular attention to entity-level controls is required because:

- These controls are presumed to have a pervasive effect on the activities of the entire company.

- Many of the control deficiencies underlying the public accounting issues of the last several years — including Enron and WorldCom — were in these areas.

A number of companies use a separate framework to supplement COSO when assessing information technology (IT) controls. COBIT[xviii] was developed by the Information Systems Audit and Control Association's IT Governance Institute in 1994 and Edition 4.0, released in December 2005, includes important updates for Section 404 and strengthens links to frameworks such as COSO. COBIT is widely used by IT audit professionals in the United States and overseas.

Additional information on internal controls may be obtained from the head of the internal audit function, The IIA, or the external auditor.

C. WHAT CONSTITUTES AN EFFECTIVE SYSTEM OF INTERNAL CONTROL AS IT RELATES TO THE REQUIREMENTS OF SECTION 404?

Management needs to determine whether the system of internal control in effect as of the date of assessment provides reasonable assurance that material errors, in either interim or annual financial statements, will be prevented or detected.

Management is able to make this assessment by:

- Identifying, assessing, and testing the design and operating effectiveness of the key controls over transactions that constitute the balances in significant accounts in the financial statements.
- Assessing whether any control deficiencies identified in the above process represent, either individually or in aggregate, a more than remote likelihood of a material error (a "material weakness").

If the scope and quality of management's identification, assessment, and testing of key controls is sufficient to address all major risks to the integrity of the financial statements and no material weaknesses are identified, then management usually will be able to assess the system of ICFR as effective. However, the presence of a single material weakness precludes management from making such an assessment. This is appropriate, as a material weakness, by definition, indicates that the system of internal control does not provide reasonable assurance regarding the reliability of the financial statements.

Each of the above is discussed in more detail in the following sections.

D. WHO IS RESPONSIBLE FOR INTERNAL CONTROLS?

Sarbanes-Oxley, both Section 302 and Section 404, makes it very clear that management — specifically the CEO and CFO — is responsible for the adequacy of internal controls. The certification by these officers required by Section 302 states:

> "(4) The signing officers —
> (B) Are responsible for establishing and maintaining internal controls.
> (C) Have designed such internal controls to ensure that material information relating to the issuer and its consolidated subsidiaries is made known to such officers by others within those entities, particularly during the period in which the periodic reports are being prepared.
> (D) Have evaluated the effectiveness of the issuer's internal controls as of a date within 90 days prior to the report.
> (E) Have presented in the report their conclusions about the effectiveness of their internal controls based on their evaluation as of that date."

Although the CEO and the executive team as a whole may look to the CFO for overall leadership and accountability for financial reporting, other parts of the organization have a significant part to play. For example, the system of ICFR typically includes processes in the procurement, inventory management, manufacturing, sales, and information technology functions, not all of which report to the CFO.

Responsibility for the system of internal control within a typical organization is a shared responsibility among all the executives, with leadership normally provided by the CFO.

The audit committee of the board of directors has a very significant role in a company's system of internal control, which it performs on behalf of the full board and ultimately the shareholders. Specifically, the members:

- Provide oversight of management. Both management and the external auditor are required to consider the effectiveness of the audit committee as part of their assessments of ICFR. COSO describes their role:
  "Management is accountable to the board of directors, which provides governance, guidance, and oversight. Effective board members are objective, capable, and inquisitive. They also have a knowledge of the entity's activities and environment, and commit the time necessary to fulfill their board responsibilities. Management may be in a position to override controls and ignore or stifle communications from subordinates, enabling a dishonest management which intentionally misrepresents results to cover its tracks. A strong, active board, particularly when coupled with effective upward communications channels and capable financial, legal, and internal audit functions, is often best able to identify and correct such a problem."
- Provide direction and oversight of the work of the external auditor, who is appointed by, and reports directly to, the audit committee.
- Direct and oversee the performance of the internal audit function, which typically reports to the audit committee.

The external auditor is engaged by, and is directly accountable to, the audit committee, a requirement of Sarbanes-Oxley. Through their audit of the annual financial statements, review of the interim financial statements, and audit of the system of internal control over financial reporting, they provide the audit committee, board of directors, investors, and management with assurance of the reliability of the financial statements. Although the external auditor provides assurance to the audit committee relative to the financial statements filed with the SEC, management is not permitted to place reliance on their work for purposes of Section 404. Management, instead, must have a system of internal control that is sufficient without relying on the external auditor.

By contrast, the internal audit function is considered part of an entity's internal control system, even though it also is directly accountable to the audit committee in most public companies. Although the chief audit executive (CAE) may report to a senior executive for administrative matters, he/she should report functionally to the audit committee. The internal audit function provides assurance to both management and the audit committee regarding the effectiveness of all aspects (i.e., not only financial, but also operational effectiveness and compliance) of an organization's system of internal control, risk management, and governance practices.[xix] Its activities are considered part of the Monitoring layer of the system of internal control and therefore are included in both management's and the external auditor's assessment. COSO describes their work:

> "Internal auditors play an important role in evaluating the effectiveness of control systems, and contribute to ongoing effectiveness. Because of organizational position and authority in an entity, an internal audit function often plays a significant monitoring role."

The audit committee can and should rely on the assurances of management, internal auditors, and the external auditor in forming its own assessments and in approving financial statements for filing with the SEC.

Additional information on the roles and responsibilities of each participant can be obtained from the company's CAE or The IIA.

E. WHAT IS THE SCOPE OF MANAGEMENT'S ASSESSMENT OF THE SYSTEM OF INTERNAL CONTROL OVER FINANCIAL REPORTING?

Management is actually required to provide more than one assessment of internal controls in its filings with the SEC. One is required by Section 302 and is included in quarterly as well as annual financial reports. The other is required by Section 404 and is only included in annual reports.

When the SEC developed the detailed rules for implementing Section 302[xx], it required the CEO and CFO to make a number of statements relative to internal controls (the Section 302 certification) and the company to include in its annual and quarterly financial statements an assessment of its "disclosure controls" and procedures, a new term not actually mentioned in the Sarbanes-Oxley Act. The SEC defined *disclosure controls* as:

> "…controls and other procedures that are designed to ensure that information required to be disclosed by the company in its Exchange Act reports is recorded, processed, summarized, and reported within the time periods specified in the Commission's rules and forms. Disclosure controls and procedures include, without limitation, controls and procedures designed to ensure that information required to be disclosed by the company in its Exchange Act reports is accumulated and communicated to the company's management (including its principal executive and financial officers) for timely assessment and disclosure pursuant to the SEC's rules and regulations."

A simple and practical definition of the scope of Section 404 is that it addresses everything in the GAAP-based interim and annual financial statements and related notes that are filed with the SEC.[xxi] Disclosure controls include this and more.

The scope of disclosure controls is broad, including all "information required to be disclosed by the company in its Exchange Act reports." These reports include not only the financial statements and related footnotes, but nonfinancial information as well. It is important to note that disclosure controls cover not just the quarterly and annual financial statements filed on Forms 10-Q and 10-K, but also notifications of material events filed on Form 8-K or other current reports.[xxii] By contrast, Section 404 only relates to the financial information required to be included in filings with the SEC.

Disclosure controls include, in their entirety, all the Section 404 internal controls over financial reporting. Although the SEC in its early publications indicated that there would be significant overlap, in practice there are no key internal controls over financial reporting for Section 404 that are not part of disclosure controls.[xxiii] On the other hand, there are significant areas covered under disclosure controls that are not part of ICFR. Examples of the latter include Management's Discussion and Analysis (MD&A) and the timely notification to investors using Form 8-K of material events.

Companies need not only (1) internal controls to ensure the completeness and accuracy of the financial information included in their filings with the SEC, but also (2) internal controls to ensure the completeness, accuracy, and timeliness of nonfinancial information filed with the SEC. The combination of the two represents disclosure controls.

As a result:

- The assessment of disclosure controls can be that they are not effective, even though internal controls are effective; for example, due to issues surrounding timely notification of material events to investors.
- If internal control over financial reporting is assessed as ineffective, disclosure controls cannot be considered effective[4]. This is because the financial information included in the filings with the SEC is the most critical part of those reports.

Section 302's requirements include, as mentioned above, a certification by the CEO and CFO and an assessment of its disclosure controls. The certification includes the following statements that relate to internal controls:

"4. The registrant's other certifying officer and I are responsible for establishing and maintaining disclosure controls and procedures (as defined in Exchange Act Rules 13a-15(e) and 15d-15(e)) and ICFR (as defined in Exchange Act Rules 13a-15(f) and 15d-15(f)) for the registrant and have:

(a) Designed such disclosure controls and procedures, or caused such disclosure controls and procedures to be designed under our supervision, to ensure that material information relating to the registrant, including its consolidated subsidiaries, is made known to us by others within those entities, particularly during the period in which this report is being prepared;

(b) Designed such internal control over financial reporting, or caused such ICFR to be designed under our supervision, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles;

(c) Evaluated the effectiveness of the registrant's disclosure controls and procedures and presented in this report our conclusions about the effectiveness of the disclosure controls and procedures, as of the end of the period covered by this report based on such evaluation; and

(d) Disclosed in this report any change in the registrant's ICFR that occurred during the registrant's most recent fiscal quarter (the registrant's fourth fiscal quarter in the case of an annual report) that has materially affected, or is reasonably likely to materially affect, the registrant's internal control over financial reporting; and

"5. The registrant's other certifying officer and I have disclosed, based on our most recent evaluation of internal control over financial reporting, to the registrant's auditors and the audit committee of the registrant's board of directors (or persons performing the equivalent functions):

(a) All significant deficiencies and material weaknesses in the design or operation of ICFR which are reasonably likely to adversely affect the registrant's ability to record, process, summarize, and report financial information; and

---

[4] *Management may want to consult with SEC counsel on this matter. As discussed in note xiii in the back of this guide, the SEC and certain SEC counsel believe (and the authors concur) there are aspects of ICFR that are not included in disclosure controls. However, we believe all key controls for Section 404 will be included. An analysis of filings with the SEC in year one of Section 404 identified that 94 percent of the companies that assessed their ICFR as ineffective also assessed their disclosure controls as ineffective.*

(b) Any fraud, whether or not material, that involves management or other employees who have a significant role in the registrant's internal control over financial reporting."

Clearly, there is a need to assess the adequacy of ICFR at interim periods to support the Section 302 certification, as well as the annual assessment required by Section 404.

There are some major differences between the annual Section 404 assessment and that required for the interim Section 302 assessments:

- The interim assessment[xxiv] for Section 302 is not audited by the external auditor.
- There is no requirement (at present) that the rigor and formality required in practice for Section 404 is repeated each quarter for the Section 302 assessment. For example, there is no requirement that management test all, or even a significant portion of its key controls each quarter. In addition, management's Section 302 process is not required to follow a recognized internal controls framework.

However, prudence suggests that management:

- Has a reasonably formal, documented process for making the quarterly assessment that is included in the 10-Q and supports the Section 302 certifications.
  - The authors suggest that this can be included in the activities of the company's disclosure committee, which most of the larger companies have established.
  - The process should include the assessment of all internal control deficiencies known to management, including those identified not only during management's assessment process, but also any identified by either the external auditors in their Section 404 work or by internal auditing in its various audit activities.
  - As discussed below, the system of ICFR has to provide reasonable assurance with respect to the quarterly financial statements as well as the annual statements. The quarterly assessment is against a lower — typically one quarter the size — determination of what constitutes material.
  - The process and results should be reviewed and discussed with the CEO and CFO to support their Section 302 certifications.
- Confirms that the external auditor does not disagree with management's quarterly assessment.
  - Understands (which requires an appropriate process to gather the necessary information) whether there have been any major changes in the system of internal control during the quarter. A major change can include both improvements and degradations in the system of internal control. Although Section 302 only requires the disclosure in the 10-Q of a *material weakness* and the communication to the audit committee of a material or significant deficiency, the *correction* of a *significant* deficiency is likely to be considered a major change and, if so, should be disclosed.

Management's assessment for Section 404 is as of year-end, so there may be a temptation to wait until late in the year before starting the Section 404 program. However, there are important reasons for considering the program a continuing, year-round process and starting early each year:

- Significant resources are required for testing that may be in short supply later in the year. Testing can be performed throughout the year, spreading the resource burden. Note: if controls are tested early in the year, management needs to perform an update procedure to "roll forward" the results to year-end.
- If there are issues relative either to the design or the consistent operation of the controls (in other words, exceptions will be identified during the testing), management will have time to make changes and retest successfully before year-end.
- The external auditors often have a policy requiring they start their testing only *after* management has tested and assessed the individual controls as effective. The earlier the external auditors perform their testing, the more time there is for management to remediate any issues and retest.

As explained above, spreading the testing provides management with improved assurance supporting the quarterly Section 302 certification and assessment of disclosure controls.

1) RISK ASSESSMENT

As discussed above, Section 404 only relates to the GAAP-based, interim and annual financial statements and related notes included in filings with the SEC.

In defining the detailed scope for management's assessment, a risk-based and top-down approach is recommended. This involves identifying:

- The general ledger accounts that make up each line in the filed financial statements. For example, accounts payable is normally a single line in the financial statements, although it represents a group of related general ledger accounts.
- For each of the above, which accounts are considered significant.
- The financial statement assertions relevant to those accounts and material to the investor.
- Locations to include in scope.
- The business processes that process transactions into the significant accounts at in-scope locations.
- The key transactions representing balances in the above accounts.
- The key controls over those transactions that ensure the financial statement assertions are achieved.

Because so much will depend on whether the system of internal control provides reasonable assurance that a material error will be either prevented or detected, the place to start is a definition of *material error*.

There is guidance in the accounting and auditing literature on this topic that is lengthy (and not repeated here), but comes down to a fairly simple test: what would be material to the reasonable investor in making an investment decision in the company's securities. It is preferable if the external auditor agrees with management's determination of what constitutes a material error, so early discussions should be held. The external auditor may indicate that only a preliminary determination may be made, as facts may change before the end of the year.

The determination of a material a error for Section 404 should consider:

- The level of error that would be material to the full year's results if it affects the income statement.[xxv]
- Not all errors affect the profit and loss (P&L), only the balance sheet. In a few cases, the errors are in the disclosures (e.g., footnotes or earnings per share (EPS) calculations). The specific facts and circumstances of these errors will have to be assessed.
- In all cases, a bright-line definition must be tempered with an assessment of what a reasonable investor might conclude. It is easy to rush to judgment and label an error material that would have no effect on any investor's assessment of the company.

This determination of what would be material for the annual and also for the interim financials should be made by technical accounting personnel, after discussion with the external and internal auditors. The determination will consider not only quantitative but qualitative factors.

Having decided on a materiality level for the full year's P&L, management needs to determine how and where an error could occur. The financial statements are examined to determine in which accounts and disclosures there is the possibility of a material error. These are considered "significant accounts."

KEY POINTS

WORKING WITH EXTERNAL AUDIT

Management should work closely with the external auditor at every stage of Section 404 process.

Management's planning materiality level will influence the external auditor's own level, which can have implications on the extent of testing and related costs.

Accounts that are small and highly unlikely to contain an error of a material amount can be excluded from the scope for Section 404. Most companies set a threshold for identifying these "small" accounts, called *planning materiality*. This is a convenient, but not required, step in the process.

Management should work closely with the external auditor at every stage of the Section 404 process, and planning materiality is an important agreement to make. Although the external auditors may set a planning materiality for their own purposes that is higher than management's, they will consider management's level when they form their opinion on whether management's Section 404 process is adequate. In addition, management's level will influence the external auditors' own level, which can have implications on the extent of testing and related costs (both for management testing and external auditor fees).

Once planning materiality has been set and agreed upon, management should identify the general ledger accounts that they believe can be excluded, as they fall — or are expected by year-end to fall — below that level[xxvi]. The decision should be reviewed carefully to ensure there are no qualitative reasons (e.g., because of known risks) that indicate one of these smaller lines should be retained in Section 404 scope[5]. Care needs to be taken with accounts that can fluctuate significantly or are anticipated to change before year-end.

The scope of Section 404 extends to the footnotes that are part of the financial statements. Management needs to perform a risk assessment on all of the notes to determine which are significant and the nature and magnitude of an error that would be considered material to the investor. That determination may affect the selection of which accounts to include in scope, perhaps including some accounts that are below the agreed planning materiality.

Management can then review each remaining account to determine whether additional accounts can be excluded — because although they exceed planning materiality, by their nature it is unlikely that a material error will be made. An example could be an asset or liability whose value has not changed and is not expected to change, such as a long-term investment or loan.

Materiality, planning materiality, and the accounts in scope should be assessed at least quarterly, or when there are material changes in the business, to ensure there is no need to add or remove areas from scope.

The external audit profession has identified a number of financial statement assertions that may be applicable to the selected general ledger accounts. Management needs to define which assertions are applicable to which accounts, as later in the process, they will have to verify there are key controls to ensure these assertions are achieved. The assertions described in AS 2, which are recommended but not mandatory (if they are not used, management needs to document how they have ensured all potential risks of material error in each significant account are addressed by appropriate key controls) are as follows:

- **Existence or Occurrence** addresses whether assets or liabilities exist at a given date and whether recorded transactions have occurred during a given period.
- **Completeness** addresses whether all transactions and accounts that should be presented in the financial statements are so included.
- **Valuation or Allocation** addresses whether asset, liability, equity, revenue, and expense components are included in the financial statements at appropriate amounts.
- **Rights and Obligations** relates to whether the rights and liabilities are the obligations of the entity at a given date.
- **Presentation and Disclosure** addresses whether particular components of the financial statements are properly classified, described, and disclosed.

The majority of companies have operations in multiple locations, and it may be possible to exclude some of those locations from scope on the basis of materiality. Alternatively, some of the processes at those locations may be excluded. The PCAOB included in AS 2 (as Appendix B) a process for making that determination that has been widely accepted — although each company should

[5] The SEC emphasized this in its May 2005 report: "When identifying significant accounts and related significant processes in order to determine the scope of its assessment, management generally will consider both qualitative and quantitative factors. Qualitative factors include the risk associated with the various accounts and their related processes …
In addition to considering qualitative factors, the staff understands that management generally establishes quantitative thresholds to be used in identifying significant accounts subject to the scope of internal control testing. The use of a percentage as a minimum threshold may provide a reasonable starting point for evaluating the significance of an account or process; however, judgment, including a review of qualitative factors, must be exercised to determine if amounts above or below that threshold must be evaluated."

confirm that it is suitable for the company's own unique situation. The process is summarized below.

- Are there any locations that are individually significant because of their size, specific risks, or other reasons?
- Are there any locations that, when aggregated with similar locations, should be included because they share common processes or otherwise are similarly affected by a controls deficiency?
- Review the general ledger accounts determined to be in scope and identify from which locations the balances are derived.
- For all the in-scope general ledger accounts, select a combination of the locations that were identified under Steps 1 or 2 above such that the greater part of the balance in each account will be covered (a useful, but informal, rule of thumb is that management should cover sources representing at least 70 percent of balances of in-scope accounts) or at least provide sufficient coverage that the risk of a material misstatement is addressed.
- Review the selected general ledger/location combinations to ensure they are reasonable based on risk. They should represent the areas where a material error is at least reasonably possible, and exclude any areas where such an event is not likely.

The balances in the significant accounts are the result of transactions that flow through a number of business processes. For each account and location combination, the key business processes now need to be identified.

The authors recommend that a further level of detail be considered, identifying which transactions make up the preponderance of the account balances. That will enable a focus on those material transactions together with the related processes and controls, and the exclusion of immaterial transactions that flow into significant accounts. For example, the significant account for depreciation may include not only the depreciation of plant and equipment, but also the depreciation of company vehicles. For most companies, depreciation of the small number of company vehicles is not material either to the P&L or the balance sheet and should be excluded from scope for Section 404.

At this point, management has identified:

- The significant general ledger accounts and notes to be included in scope, and the related financial statement assertions.
- At which locations the controls and processes related to those accounts will be assessed and tested.
- The business processes and material transactions that make up the balances in those accounts.

2) PROCESS AND CONTROL DOCUMENTATION

The key business processes and, especially, the material transactions and related controls now need to be documented. There are various techniques and documentation styles for completing the documentation. However, management needs to complete documentation that:

- Enables a reasonably knowledgeable individual (this person does not have to be an expert with experience in the area but should have some knowledge of the company or its business) to understand the process.

- Provides context for the key controls such that a reasonable person would understand their function.
- Details the operation of key controls, such as identifying who is performing the control, when the control is operating and at what frequency, how the control is performed, what evidence exists that the control has been performed, and what reports are used in the operation of the control. It is important to agree with the external auditor on the quality standards to be established for control documentation.
- Overall, enables a reasonable person to have a basis upon which to assess the design of the controls: Are the controls identified and documented sufficiently to either prevent or detect a material misstatement? This is discussed further under "Key Controls."

Management should remember that the external auditor will be assessing whether management's process for making its assessment for Section 404 is adequate. A significant piece of that is whether there is adequate documentation of the processes and controls on which to base an assessment.

It is critical to establish a change management process to ensure that documentation is kept up-to-date as processes and controls change. The business does not stop just because of Section 404 requirements. A sound change management process for Section 404 will likely have the following attributes:

- The process is well known to all business process owners.
- Changes to business processes, including computer systems, are identified, and the documentation is updated promptly.
- Changes to key controls are identified and assessed promptly to ensure the potential impact on Section 404 assessment and testing is understood.
- Planned changes, especially those planned for late in the fiscal year, are discussed to ensure the impact on the Section 404 assessment is understood. Consideration is given to delaying the change until after year-end.

3) KEY CONTROLS

Although referenced in PCAOB documents (including the Nov. 30, 2005 report), there is no commonly accepted definition for a key control. The authors support the following, which we believe is consistent with PCAOB published guidance:

> *A key control is a control that, if it fails[6], 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[xxvii]. In other words, a key control is one that provides reasonable assurance that material errors will be prevented or detected timely .*

[6] *The failure could be individual or combined with other controls that are likely to fail at the same time. Although the failure of one control may not be likely to result in a material misstatement, several may fail at the same time, increasing the risk of a material misstatement to more than remote. This scenario is called* aggregation *in the literature. The key is that the controls have to be* likely *to fail at the same time, for example, because they are performed at the same time, by the same people, or using the same computer system.*

F. DEFINING THE DETAILED SCOPE FOR SECTION 404

Careful identification of key controls is important to an efficient and effective Section 404 program. An overly conservative approach, where too many controls are defined as "key," will result in excessive time and resources testing controls that are not critical to the assessment. On the other hand, if too few controls are identified, this may result in a significant problem when the external auditor identifies, and management then agrees with, the need for additional key controls.

Technically speaking, management may be considered not to have an adequate basis for its assessment unless adequate evidence is obtained that all key controls are operating effectively. These newly-identified key controls may not have been addressed. Management may be able to recover by documenting and testing the controls, but that is likely to be later in the year. There is a risk of insufficient time to demonstrate, through testing, the effectiveness of key controls identified late in the process.

It is important to note that there is no generic "laundry list" of what will always be considered "key controls" and, due to differences in systems, procedures, business environments, and models, sound professional judgment is required during the identification process. Management should also give due consideration to the views of the external auditors and ensure they are comfortable with the process management uses for identifying key controls.

Controls may be preventive or detective — either prevent errors or detect their occurrence. Some experts include the determination of whether controls are preventive or detective in their process to identify key controls, because preventive controls are seen as stronger. However, management should recognize that an efficient and effective system of controls will use a combination of both, and the authors do not consider it critical to focus on whether controls are one or the other. Rather, management should instead focus on whether the controls in place are sufficient to ensure there are no misstatements of the financials and are appropriate in terms of management of business risk.

There are two schools of thought when it comes to identifying key controls:

- In the first, risks that may prevent the financial assertions from being satisfied are listed. Then, the controls that address those risks are identified. The benefit of this approach is that it is relatively straight-forward and familiar to most experienced auditors. It is also the approach recommended in PCAOB's AS 2. However, the risk is that the list of risks may not be complete.
- The second approach looks at the transactions that flow into the significant accounts and identifies the controls that assure the transactions are completely and accurately processed and recorded, and that only valid transactions are processed. The second approach, which has been adopted less frequently, includes controls that assure the safeguarding and existence of the assets and the presentation of account balances in the financial statements. The benefit of the second approach is that it provides more assurance that all the controls are addressed. However, it is more complex.

Both approaches have merit. Management should make a choice based on which is more consistent with the experience and training of the individuals managing the project, after consultation with the external auditor.

The majority of companies use a process that starts with the significant general ledger accounts by location, defines the relevant financial assertions for each, and then lists all the risks to achievement of the assertions. Finally, the key controls — those required to address each risk such that a material error is not likely — are identified. For example, the process may start with "Cash" at the headquarters location and identify "Existence" as one of the assertions to be achieved. The bank reconciliation is identified as the key control that addresses that assertion.

It is important to ensure the list of risks is complete. The external auditor may have a list of standard or common risks for different types of accounts and the internal auditor can assist with a review of the list of risks. An additional source, if the company uses specialized Section 404 software, is the vendor of the software, who typically has templates that management may use.

For companies with complex reserve calculations (e.g., inventory or product warranty reserves), attention should be given to ensuring there are key controls around all the information used in the reserve calculation (e.g., estimates of future sales prices, customer demand, etc.).

The alternative method also starts with the significant accounts by location, but differs by identifying the material transactions flowing into those accounts. For each material transaction, key controls are identified to ensure the transactions are completely and accurately recorded (including calculations) and that only valid transactions are recorded. In addition, key controls are identified to ensure the appropriate presentation of the significant accounts in the financial statements, and that all assets in significant accounts are safeguarded. For example, cash at the headquarters location is identified as a significant account and location. The bank reconciliation is identified as a key control because it helps ensure both the completeness and accuracy of cash recordings.

Both of these methods can result in the identification of too many controls, including duplication of controls, unless reviewed carefully. A number of reasonable tests can be performed to validate the list of key controls, including:

Highly Persuasive Test

Does the control have one or more characteristics that are highly persuasive to determine that it is a key control?

- Operating management considers it key, even if they are unable to link it to a risk or assertion.
- Common sense indicates it is a key control.
- The control addresses an assertion or risk that is not addressed by other controls.
- It directly addresses a section in the Sarbanes-Oxley legislation, for example, the code of ethics or whistle-blowing procedures.
- It describes a key role in monitoring the effectiveness of controls across the entity (e.g., internal auditing or the audit committee).
- The external auditor considers the control as key.

KEY POINTS

VALIDATING KEY CONTROLS

Highly Persuasive Test: Does the control have one or more characteristics that are highly persuasive to determine that it is a key control?

Acid Test: 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?

F. DEFINING THE DETAILED SCOPE FOR SECTION 404

Acid Test

This test needs to be applied to each key control, but with caution to ensure management does not end up with an overly conservative list of key controls.

- 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 those 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. (Although it is management's responsibility to determine which are its key controls, the external auditor is responsible for assessing management's Section 404 process[xxviii]. In addition, it is more efficient if management and the external auditor can agree on, and then test (the same controls — as it becomes more likely that the auditor can place maximum reliance on management's testing.)

When discussing the results of the acid test with the external auditor, management may refer to the PCAOB's May 16, 2005 guidance — specifically, its Staff Questions and Answers (Number 38) relative to risk assessment and a top-down approach to their audit: "A top-down approach prevents the auditor from spending unnecessary time and effort understanding a process or control that does not affect the likelihood that the company's financial statements could be materially misstated … This approach also helps the auditor to identify and eliminate from further consideration accounts, disclosures, and assertions that have only a remote likelihood of containing misstatements that could cause the financial statements to be materially misstated."

Once management has completed this process, it is prudent to consider the risk of a failure of one or more of the key controls. Points to consider include:

- Are there any higher level controls (e.g., analytical or other monitoring reviews, including executive dashboards and the use of key metrics) that would detect the failure of a key control and/or a material error resulting from a controls failure? For example, if the company measures inventory turns on a regular basis and investigates trends and significant fluctuations, that control is likely to detect a material error in inventory valuation or in the calculation of cost of sales. In such cases, it may be prudent to consider these as key controls.
- Are there additional controls, especially in higher risk areas, that should be added as key controls because they would compensate or mitigate the effects of a failure of a key control? An example might be where the key control — perhaps a review of major fixed asset additions against approved capital expenditure forms — is performed at a regional level. A backup key control may be added: the local review and approval of capital expenditures.

- If the number of key controls is low, it becomes more critical to:
  - Ensure operating management is aware of which controls are key and how important it is to ensure they are operating effectively throughout the year. Operating management may want to monitor performance through supervision and spot testing more carefully.
  - Perform testing early, to provide time for remediation and retesting.
  - Ensure any deficiencies are corrected promptly.

4) IDENTIFYING IT CONTROLS

This is an important area, and the management team should ensure sufficient attention is given to the identification of key IT controls by individuals with a broad understanding of the business and the overall Section 404 project. Experience has shown that, unless managed carefully, significant problems can arise.

- Failures to effectively link work performed on IT controls to the overall, top-down Section 404 risk assessment process and identification of key controls are common. Some external and internal auditors believe specific generic controls should exist in every organization, but that belief is often based on an assessment of technical risk that may not consider the existence of manual controls or the risk of error in the financial statements. It is critical to have a good understanding of why computer systems are important and the impact a failure in general controls may have.

  In other words, IT controls should be the result of a top-down approach. The PCAOB made the following comment in the November report:

  > "Most of the audit engagements reviewed by the Board's inspectors did not use a top-down approach … Auditors who used a bottom-up approach often spent more time and effort than was necessary to complete the audit."

- The scope of work may be more than required, impacting the cost of the project.

KEY POINTS

IDENTIFYING IT CONTROLS

The management team should ensure sufficient attention is given to the identification of key IT controls by individuals with a broad understanding of the business and the overall Section 404 project.

Failures to effectively link work performed on IT controls to the overall, top-down Section 404 risk assessment process and identification of key controls are common.

It is important to recognize that these comments apply equally to management (perhaps more so, as the auditors typically follow management's identification of key controls).

The authors recommend a process for identifying IT controls to document, assess, and test as follows:

1. Ensure that a single team manages the entire process, including IT-related controls, to ensure a single risk assessment is made. All the work should be driven with a common understanding of the need to focus on risk of material error in the financial statements.

2. Agree on the general approach and on the results of each key stage with the external auditor. It may be possible to realize savings in audit fees through effective joint planning.

3. When defining the key business processes, identify the applications used in those processes to handle the flow of material transactions.

4. When identifying key IT controls, recognize that:
   - Some key business controls are fully automated, for example the calculation of interest for banks or updating the correct general ledger account. These are clearly automated controls.
   - Some controls are partly automated. For most companies, a large number of controls are of this type, where the individual performing the control relies on a computer report or information on a computer screen.
   - Other controls are fully manual, for example the inspection of incoming materials for quality.

5. Key controls that are fully automated need to be documented to the same standard as manual controls. To facilitate testing, attention should be given to documenting the control operation in some detail on page 37.

6. Key controls that are only partly automated need to be examined carefully. If the manual portion of the control is sufficient to detect an error in the automated part (e.g., the computer report) then the control can be considered entirely manual, because no reliance is being placed on the computer system. An example of this is the bank reconciliation, where the control uses reports from the general ledger system listing the cash balance and the various transactions in the month. The reconciliation to the bank statement provides assurance that the reports are correct.

   However, if the automated part of the control is not assured by the manual part, then it will have to be tested as an automated control, as described on page 37.
   - An example of a report that requires further testing is a report of all transactions greater than a defined dollar limit. The individual reviewing and taking action on this report cannot know that the report is complete, and lists all items over the threshold. Therefore, the report should be tested as an automated control.

   Key controls using some form of end-user computing, including spreadsheets or Business Objects reports, may require special attention, as described further in Section G of the is guide[7].

7. Part of the strategy for testing automated controls, whether testing those identified in No. 5 or No. 6 above, will be reliance on general computer controls.

[7] *Some of the external audit firms emphasize a concept called "key reports," commonly described as reports used in key controls. However, the authors believe the only key reports that need to be examined as automated controls are those where an error would not be detected in the normal course of the manual part of the control.*

When automated controls are identified, management should identify, document, assess, and test the controls over the related applications. In addition, consideration should be given to any other applications involved in processing material transactions. If the identified key controls would not prevent or detect inappropriate processing or the unauthorized change of data related to those applications, and therefore could result in a material error in the financials, they should be included in the ITGC scope. In other words, the ITGC scope should address applications where a failure in the related ITGC is reasonably possible and could (again, there's a reasonable possibility) result in a material misstatement of the financials.

If an application processes material transactions but a failure in ITGC, which includes security, is not at least reasonably likely to result in a material error, then that application can be excluded from the ITGC scope for Section 404 purposes. (Note: there may be good reason to assess and test ITGC for operational and risk management purposes, even if there is no need to do so for Section 404).

Broadly speaking, information technology general controls (ITGC) provide assurance that applications are developed and subsequently maintained, such that they provide the functionality required to process transactions and provide automated controls. They also assure the proper operation of the applications and the protection of both data and programs from unauthorized change.

8. The balance of the strategy for testing automated or partly automated controls is the specific testing of the automated controls. However, before developing the plan for specific automated controls testing, management should consider *benchmarking*.

Where there are good change management controls within ITGC over an application, management may decide to test only a sample of automated controls each year. The principle, called "benchmarking," is described in the PCAOB document issued May 16, 2005[xxix]. The principle needs to be applied to each automated control in turn, examining whether: (a) the software has been changed since the last time it was tested, (b) whether there are sound change management processes and controls relative to the software, and (c) whether the control is of such significance that risk demands it be tested every year.

In principle, when a company has invested in effective and consistent change management controls, it should have increased assurance that the software (including automated controls) will provide the required functionality on a consistent basis. Management should consider this when planning which automated controls to test. Even if no changes have been made, it is advisable to test at least a sample.

Testing of automated controls is discussed further on page 37.

5) IT GENERAL CONTROLS

ITGCs can be extensive and can include a significant number of controls relative to the development, maintenance, and operation of applications and infrastructure (e.g., operating systems and databases), as well as the security of the computer network, applications, and data. Due to ITGC's technical nature, the changing threats to network security, and cost constraints, it is difficult for IT management to design and operate controls that are fully effective, and IT auditors will usually find some deficiency. As a result, IT management at many organizations has incurred additional costs, including personnel, to ensure key ITGC controls are designed and operated adequately.

KEY POINT

IT GENERAL CONTROLS

Failure to define the scope of ITGC carefully 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. On the other hand, deficiencies in ITGC can result in material error if not mitigated or compensated for by controls in other areas.

Failure to define the scope of ITGC carefully 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. On the other hand, deficiencies in ITGC can result in material error if not mitigated or compensated for by controls in other areas.

- Deficiencies in application change management can imply the functionality in key automated controls is at risk. Even if the automated control is tested, there is reduced assurance that the control continues to operate as tested.
- Security weaknesses can increase the risk of unauthorized changes to data, bypassing normal transaction controls, or to applications, putting automated control functionality at risk.
- Computer operations control issues can imply that backups are in question and, if an application fails, errors could be introduced during the recovery. There could also be a risk that applications are not run properly, putting the functionality of automated key controls or the integrity of data (if interfaces are affected) at risk.

We recommend that management identify a set of control objectives for ITGC that can be applied to each in-scope application. The latter should include all applications that contain key automated controls, as well as all applications that process material transactions where an error in the processing could result in an undetected material error in the financials.

The control objectives should address each sub-area of ITGC:

- Development or major enhancement of new applications.
- Maintenance of existing applications.
- Application user management, such as approval of new user IDs and removal of user IDs for terminated or transferred employees and contractors.
- Management of change to the IT infrastructure (e.g., operating systems and database management systems).
- Computer operations (e.g., execution of applications; monitoring of and responding to application errors; backups of applications and data; and computer room security).
- Network security.

- General management and organization of IT (e.g., segregation of duties and the role of IT security within the organization).

Management then will identify which of these control objectives for each of the in-scope applications represent a risk that (a) is at least reasonably likely to occur, and (b) if it occurred is at least reasonably likely to result in a material error in the financials. For example, in some organizations, failures to achieve objectives related to anti-virus protection or intrusion detection may not present a risk to the proper operation of an SAP application, and thus may not represent a risk to the financial statements. Such failures may be deemed to represent only a risk of business disruption, not a risk of undetected change to SAP data or application functionality.

As with business processes, ITGC processes need to be documented and controls identified that will satisfy the control objectives identified above. Management should identify and test only those key controls necessary to achieve the control objectives for in-scope applications.

Detailed guidance for the efficient scoping of ITGC risks and related controls will be available in 2006 from The IIA (*A Guide to the Assessment of IT General Controls Scope Based on Risk*).

Before making the final selection of key ITGC controls, management should confirm that all meet the definition of a key control: that there is at least a reasonable risk of material error in the financial statements if any of the key ITGC controls fail. Although the effect is not direct, the ITGC key control failure might lead to a failure in one or more key business controls, or the undetected failure of application functionality.

6) TESTING AUTOMATED CONTROLS

In most cases, individuals with IT audit expertise will perform automated control testing; however, management may request IT staff to perform the tests. This is acceptable, but may not allow the external auditors to rely on management testing to reduce the scope of their work.

Each of the automated controls, including key reports, need to be tested unless benchmarking applies; an individual with IT audit experience will usually be able to identify the most appropriate test. Testing will normally consist of one or more of the following:

- Use of test data to confirm the proper operation of the control. The auditor, or IT staff with auditor review and approval, will enter transactions in the test environment and confirm the control operates as documented.
- Examination of related application code (a common technique when SAP is the application, where SAP configuration tables can be reviewed). The auditor must possess a solid understanding of the software configurations or code to perform this test.
- Use of audit software to reperform the functionality. For example, the auditor may use ACL or a Business Objects report to select and age open accounts receivable transactions and compare the results to the reports used by management.
- Manual reperformance of the control. In a few cases, where the control is not complex and the data not voluminous, the auditor may be able to recalculate totals or otherwise reperform the specific functionality of the key control.

F. DEFINING THE DETAILED SCOPE FOR SECTION 404

Unless there are concerns in ITGC that indicate otherwise, automated controls need only be tested once each year (subject to benchmarking, as discussed previous). If ITGC issues indicate there is a significant risk that unauthorized, unapproved, or untested changes may be made to the automated controls, the frequency of testing should be increased with special attention given to year-end closing processes.

7) SEGREGATION OF DUTIES AND RESTRICTED ACCESS

Segregation of duties (SOD) and restricted access (RA) controls need to be identified, assessed, and tested where considered key. Key SOD and RA controls include those that:

- Are required for an authorization control to be effective. For example, if the business control requires that all purchase orders be approved in the system by the purchasing manager, it is critical to ensure that only the purchasing manager has that capability.
- Reduce the risk of a material fraud that could be reported incorrectly in the financial statements.

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 scope for Section 404. *See the Fraud Risk Assessment section on page 42.*

Once the key controls have been identified, they should be tested. A suggested testing strategy includes:

- Test RA and SOD before mid-year to identify any issues and allow time for resolution or an explanation of how the risk is managed.
- Once management has completed all remediation, retest RA and SOD late in the third quarter or early in the fourth quarter. By then, the more significant issues will have been corrected, and the results should be positive.
- This is now an appropriate time for the external auditors to perform their tests, as management has completed their testing and obtained assurance that the appropriate controls are in place and operating effectively.

8) SPREADSHEETS AND OTHER END-USER COMPUTING ISSUES

Much has been made about the risks to financial reporting through errors in spreadsheets and end-user computing in general (including the use of Access databases and Business Objects reporting). Because spreadsheet errors have been found at a number of companies and have resulted in material errors in their financial statements, this risk needs to be acknowledged and addressed.

Risks related to spreadsheets (from hereon, that term also refers to other end-user software) include:

- Errors in the download from the company's systems, including:
  - An incomplete download (e.g., missing a general ledger (G/L) or a region).

- An out-of-date download.
- A partial download, where transmission or other errors prevented completion of the entire download.
- Use of an intermediate database (e.g., a data warehouse) that is not complete, accurate, or current.
- The incorrect population of the download data into the various cells in the spreadsheet.

- Errors in calculations, sorts, or other programmable elements of the spreadsheet.
- Use of an out-of-date spreadsheet (including use of a current spreadsheet where the calculations are not refreshed”).
- Changes to the data by the user.
- Errors in the understanding or use of the spreadsheet (e.g., where the user is not the developer and picks up the wrong total).
- Changes to the spreadsheet by another, due to poor security.

Some consultants have advised the use of specialized software in this area, and there are many products of value. However, before acquiring and implementing additional products, the authors recommend management consider the following approach:

- When a key business control includes the use of a spreadsheet, determine whether an undetected error in the spreadsheet could cause the control to fail and result in a material error in the financial statements. Determine if the spreadsheet is essential to the key control (e.g., enabling a review of an estimate) or incidental (e.g., used to list the documents being reviewed).
- Will the normal operation of the control detect an error in the spreadsheet? There are two ways this can happen:
  - The spreadsheet is used in a reconciliation process. For example, if original documents are summarized in a spreadsheet and then compared to the updated general ledger balance, an error in the spreadsheet will result in an out-of-balance condition with the general ledger.
  - The control includes user procedures to confirm the completeness and accuracy of the spreadsheet. For example, if a spreadsheet is used to analyze sales invoices by region, then confirmation of the totals to the general ledger will ensure that the download of data into the spreadsheet is complete and the formulae are properly calculating the totals.

KEY POINTS

SPREADSHEETS

If an error in the spreadsheet would not be detected in the normal operation of the control, understand where the risk is and take action accordingly.

If a walkthrough or other formal assessment of the control design is performed, it should include a discussion of how the completeness and accuracy of the spreadsheet results are assured.

- If an error in the spreadsheet would not be detected in the normal operation of the control, understand where the risk is and take action accordingly:
  - If the risk is in the download from the general ledger (or other computer system) directly into the spreadsheet, consider changing the design of the control to include a user control (e.g., a user verification of the spreadsheet totals to the general ledger).
  - If the risk is around the download of information into a data warehouse or similar (e.g., Essbase or Hyperion), consider adding controls over the download and then ensuring that the spreadsheet is balanced back to the data warehouse.

  - If the issue is that the user is entering data into the spreadsheet manually, consider adding a control to validate the completeness and accuracy of the data in the spreadsheet.
  - If the risk of error is in the calculations, consider whether the user can review the results in such a way that it will confirm the calculations are correct. If the calculations are too complex for such a review, consider replacing the spreadsheet with a report or other program developed and maintained by IT. A risk of using complex calculations in a spreadsheet is that the user may inadvertently introduce a mistake into the spreadsheet. Converting the spreadsheet into a report developed and maintained by IT will provide greater assurance that the calculations will continue to function properly, with all changes to the calculations tested and approved, assuming that IT has adequate ITGC.
  - If there is no alternative to relying on the spreadsheet and its calculations, then ensure there are controls similar to those discussed in ITGC over:
- The validity of changes to the spreadsheet, including testing and approval.
- Input (whether automated or manual) of data into the spreadsheet.
- The security of the spreadsheet, such that only valid, tested, and approved changes are made and that data is not inappropriately changed.
- The way in which the spreadsheet is used and the results interpreted. For example, there should be controls to ensure that all data is input and validated before the results of the spreadsheet are used in the key controls. In addition, there should be assurance (e.g., through documentation or user instructions) that the use of the spreadsheet is correct (e.g., the correct totals are used). An example of the latter is where a spreadsheet has multiple analyses of the data; the user should understand which analysis and which totals should be used.

When reviewing and assessing the adequacy of the design of key controls using one or more spreadsheets, the above should be considered. If a walkthrough or other formal assessment of the control design is performed, it should include a discussion of how the completeness and accuracy of the spreadsheet results are assured.

To assist the external auditor's review, and to provide a solid double-check in this area, management should consider developing an inventory of all spreadsheets that are a significant part of a key control or a critical part of the financial reporting process. The inventory should describe how assurance of the completeness and accuracy of each spreadsheet is obtained.

Testing of key controls should encompass the controls over the completeness and accuracy of the spreadsheet.

Where the spreadsheet is not assured by the normal operation of the control, management should consider performing periodic independent tests of the spreadsheet. For example, it may be included in the population of automated controls tested by IT auditors.

9) CONTROLS PERFORMED BY THIRD-PARTY ORGANIZATIONS (SAS 70 TYPE II REPORTS)

Many companies have achieved cost savings or other benefits by outsourcing selected functions, such as payroll processing, processing of stock options, or data center management. Management needs to consider these outsourced operations when developing the scope of the Section 404 assessment.[xxx] If key controls are operated by third-party organizations, they need to be assessed and tested before management can be assured that the controls are designed adequately and operating effectively.

One approach is to treat processes and related controls in the same way as management addresses processes and controls within the organization. Management needs to ensure the processes are documented adequately, identify and assess the adequacy of key control designs, then perform tests to confirm the controls are operating effectively and are consistent with the documentation. Management may find that the service provider has good documentation, in which case they need not duplicate that effort, even if the provider's documentation is not in the same format or style as the company's. Management may also be able to place some degree of reliance on any testing of its internal controls by the provider. However, management needs to consider not only the competence of the personnel performing such testing, but also the independence of the personnel from the provider's management.

Most service providers in the United States recognize their customers' need to obtain assurance over the providers' controls. Rather than have every customer send a team of auditors to document and test their controls, these providers engage a third-party auditor to perform an attest engagement under the American Institute of Certified Public Accountants (AICPA's) Statement of Auditing Standards Number 70 (SAS 70). This standard defines how independent auditors identify the controls to test, perform testing of the controls, and report the results. Reports from audits performed by independent audit firms in accordance with the provisions of SAS 70, as long as the report is what the standard calls a "type II" report (some U.S. providers only get a "type I" report, which is not sufficient for Section 404), can be relied upon by management as assurance that the providers' controls are adequate under certain conditions:

- Management needs to identify which key controls it relies on the provider to perform, review the report (which contains a description of the key controls tested), and confirm that the design of the control is sufficient to meet management's control objectives.
- The company typically will need controls that work with those at the service provider. For example, the company should have controls to ensure all transactions are transmitted to the provider for processing. Management should ensure these controls work effectively in combination with the provider's. Most SAS 70 reports include a description of the controls the provider expects its customers to have. This is a section management should review carefully.
- Management should review the report carefully to verify the testing is sufficient to ensure the adequacy of the controls on which they will rely, and then assess the results reported.

If the SAS 70 report identifies deficiencies, management needs to determine what impact the deficiencies have on the controls at the provider on which it relies. For example, the report may identify deficiencies in Windows NT servers at an outsourced data center, while the company's software runs only on Unix servers. Management may also find that controls within the company, compensate, or at least mitigate, the deficiencies.

Service providers do not always provide assurance that any deficiencies will be corrected and retested before their customers' year-ends. Although the authors believe management should work with the provider to include a commitment to address deficiencies in the contract, the provider may not be responsive. Therefore, management should ensure excellent communications are in place to provide as much notice as possible of potential audit issues.

Outside the United States, providers often do not offer a SAS 70 type II report. Management needs to identify this early and plan accordingly. One option is to pay the provider to obtain such an audit, and another is to develop controls within the company that will address any risks to the financial statements. Finally, management may decide to switch providers to one that provides a SAS 70 type II report.

Additional information on a SAS 70 type II report can be obtained from the external auditor.

10) FRAUD RISK ASSESSMENT

The concept of a fraud risk assessment is one that is frequently misunderstood, even though PCAOB AS No. 2[xxxi] clearly states:

"The auditor should evaluate all controls specifically intended to address the risks of fraud that have at least a reasonably possible likelihood of having a material effect on the company's financial statements." [xxxii]

The key to an efficient consideration of fraud is to focus on fraud schemes that could result in a material misstatement of the financials[8]. Many thefts and frauds, Although significant and important to prevent — or at least detect — promptly, are unlikely to result in a material error in the financial statements.

For example:

- The theft of inventory at a company that conducts a full physical inventory at year-end would not result in an error at year-end because a write-off will have been taken.
- The approval and payment of duplicate or excessive payments for services are recorded correctly in the financial statements: the financials correctly reflect the amounts paid, on the appropriate line of the P&L.

There are a number of detailed guides (including guides from each of the major accounting firms) on how to address fraud risk. The high-level approach is to:

- Identify the fraud schemes applicable to the company that might result in a material error in the financials if undetected. Particular attention should be given to schemes involving the management override of controls, including the approval and processing of manual journal entries.
- Identify the key controls that would either prevent or timely detect any such fraudulent activity, and confirm the adequacy of their design.
- Ensure that the identified key controls are tested.

[8] *In this discussion, fraud includes the misappropriation of assets.*

One area of focus RA and SOD. It is possible to spend a significant amount of time assessing and testing these areas, because many frauds are the result of inappropriate access and especially a combination of access capabilities (e.g., the ability to both set up a vendor and approve invoices). In addition, there are significant business reasons (including the loss of assets) for ensuring appropriate RA and SOD are in place. The key to efficient Section 404 testing for RA and SOD is carefully focusing on access abilities where a resulting fraud could mean the financials are materially misstated. If management desires, additional RA and SOD testing for purely business risk management purposes may be added to the Section 404 testing — because the cost of additional testing may be minimal. However, these non-404 tests should be identified clearly as such to the external auditor.

G. TESTING KEY CONTROLS

In theory, management has great flexibility in selecting techniques for testing key controls. They do not have to employ the same techniques (or even the same sampling criteria) as the external auditor[xxxiii]. However:

- The testing techniques should clearly provide a reasonable individual sufficient assurance that the controls are operating effectively as documented.
- If self-assessment techniques are used (these are not described here, but information can be obtained on this valuable approach from the internal or external auditor), there has to be a reasonable level of independent confirmation of the self-assessment.
- The testing needs to provide assurance that the controls are operating effectively at year-end, as that is the point in time at which the formal assessment is made. For tests performed earlier in the year, steps should be taken to update and roll-forward the results of the tests. Techniques that can be used include a limited reperformance of the earlier tests using fourth quarter transactions, or obtaining re-certifications by process owners of their key controls.
- The testing needs to be performed by competent and trained individuals. A number of organizations are requiring operating management and staff to perform regular testing of their controls. Although that may appear to be cost-effective (for example, it may free internal audit specialists to focus on valuable operational, compliance, and other control audits), management may need to provide objective reviews and retesting to ensure the tests are performed on a timely basis in accordance with quality standards and the results are reflective of actual operations. This additional review and testing might be performed by internal audit staff or a separate control testing group. Management should consider the total costs of testing and the most efficient use of resources when staffing the testing program.

This document will not explore in depth the testing techniques that are available. Management should select the approach most suitable for the organization after consultation with experts, including the internal auditor. Some of the techniques available include:

- Traditional testing of controls, which includes:
  - Performance of walkthroughs, which confirm the adequacy of the documentation as well as the design of the controls to meet the control objectives.
  - Inquiry, examination, and inspection of related documents to confirm that the control appears to be performed consistently as documented.
  - Reperformance of a sample of transactions to confirm that the control is being performed effectively.
- Continuous auditing, which includes the testing of transactions throughout the period. This is generally done with software that selects the transactions to be reviewed.
- Continuous monitoring. This technique relies on software to monitor transactions and not only identify transactions for testing, but especially to test 100 percent of the processed transactions for compliance with selected parameters. An example would be a test that identifies purchase orders issued in excess of approved requisitions. The software would report such exceptions for assessment as they occur. This technique merits attention and consideration, as several of the CPA firms are partnering with software companies to develop automated tools for continuous monitoring.
- Management self-assessment. There are several varieties of this technique, and management needs to consult with testing experts to ensure that the results of any self-assessment provide reasonable, objective evidence that the controls are operating as assessed. The risk

is that the individuals performing the assessment may not have direct knowledge of the operation of the control or may not perform a rigorous assessment, verifying the consistency of execution of the control.

Performing an annual walkthrough of key processes and controls is highly recommended. The external auditor is required to do walkthroughs, which help confirm the accuracy of the documentation as well as the adequacy of the controls. Walkthroughs by management will not reduce the requirement for the external auditors to perform their own walkthroughs[xxxiv], but they will detect errors early and ensure management:

- Has a clear and current understanding of the processes and their operation.
- Can identify and correct potential issues early.
- Will perform more efficient testing, as documentation issues have been removed.
- Makes more efficient use of the external auditor's time by ensuring the currency, completeness, and accuracy of the documentation.

KEY POINTS

TESTING KEY CONTROLS

Management should always consider the total cost of the Section 404 program. That total cost includes the external auditor's fees.

Management can minimize the total costs by maximizing the degree to which the external auditors can reduce their hours through reliance on management testing

Earlier, the statement was made that management "has great flexibility in selecting techniques to use for testing its key controls." The "in theory" reservation was included because management should always consider the total cost of the Section 404 program. That total cost includes the external auditor's fees. Management can minimize the total costs by maximizing the degree to which the external auditors can reduce their hours through reliance on management testing.

It is still unclear to what extent the external auditors are able to reduce their hours through reliance on management testing when that testing is other than traditional. This is a developing area and merits continued monitoring. However, for the areas where the external auditor is required to perform independent testing and cannot rely on management testing (e.g., control areas assessed as high risk), management may be able to employ less traditional, more cost-effective methods without impacting external auditor fees.

H. ASSESSING THE ADEQUACY OF CONTROLS, INCLUDING ASSESSING DEFICIENCIES

If all the key controls are properly identified, assessed to be adequately designed, and the results of testing indicates they are all operating effectively, management is able to assess the overall system of internal control over financial reporting as effective. But, in real life, exceptions are identified in testing. A number of key controls will be deemed either to be missing, deficient in design, or not operating effectively.

Management needs to decide whether these deficiencies mean that the system of internal control does not provide a reasonable level of assurance that there will not be material errors in future financial statements.

This is achieved by assessing each control deficiency to determine whether it represents a risk of an error, including the likelihood of the error and its potential magnitude. Each deficiency is assessed to determine whether it is *material, significant,* or neither. Then, management needs to determine whether a combination of deficiencies[9] is likely to represent a risk (an *aggregated* risk) that is material or significant.

The following definitions use the terms *material error* and *inconsequential* (as discussed on page 26 and 49, respectively), and *more than remote* likelihood. The latter is related to the term *reasonable assurance*, means that there is at least a reasonable likelihood, and is generally understood to be in the 5 percent to 10 percent probability range.

- A *material weakness* is one where the likelihood is *more than remote* that an error that is *material* to the financial statements will neither be prevented nor detected within a reasonable period of time. This is more than a test that the likelihood of an error is more than remote; it is a test of the likelihood of a material error.
- A *significant* deficiency is less severe. It means that the likelihood is *more than remote* that an error that is *more than inconsequential* to the financial statements will occur.

The external audit firms have adopted a framework for assessing deficiencies[xxxiv]. This approach is important for management to consider, as it is likely to be followed by the external auditor. However, there is no requirement for management to follow precisely the same process.

Management should adopt a principles-based approach, relying on their judgment, rather than a strict rules-based approach. The PCAOB also has advised the external auditors also to rely on their professional judgment in assessing deficiencies:

> "This evaluation requires an exercise of judgment, based on an assessment of what constitutes reasonable assurance under the circumstances, not on the mechanical application of a predetermined probability formula. Inspectors observed, however, that the quest for quantitative rules of thumb in the application of the definitions described above may have resulted in some auditors exercising less judgment than the standard requires in this area. Many engagement teams used a framework developed through the collective effort of nine firms for evaluating deficiencies. That framework uses terms such as 'gross exposure,' 'adjusted exposure,' and 'upper limit deviation rate.' The statistical precision suggested by these terms may have driven auditors' decision-making process unduly toward simplistic

---

[9] *As noted earlier, the key to an aggregated risk is that the controls are likely to fail at the same time, for example because they are performed at the same time by the same people or using the same computer system.*

quantitative thresholds and away from the qualitative evaluation that may have been necessary in the circumstances.

"This evaluation framework can result in decisions that are consistent with the provisions of Auditing Standard No. 2. Further, the use of the framework promoted consistency among different audit teams within and across firms. Nevertheless, the framework is not a substitute for the professional judgment that Auditing Standard No. 2 requires. Moreover, using this framework could, in some cases, lead auditors to spend more time evaluating the severity of a deficiency than otherwise would be necessary." (Report dated Nov. 30, 2005).

Management's process must ensure the following are considered:

1. **Could there be an error in the financial statements as a result of the control deficiency?** Note that some controls may present a greater risk of business disruption or fraud that does not result in a financial statement error. If the answer is "No," the process can stop and the deficiency can be assessed as neither significant nor material. Management should further reassess whether this should remain a key control.

   With respect to deficiencies in IT general controls, management should follow the risk assessment back up the chain. They should identify what control objective is impacted and to what extent; what applications the control objective and key control addresses; what automated controls are involved; and, what risk there is of an error in the financials.

   Entity-level controls also require special handling to determine what controls and processes may be impacted. It is not sufficient to simply say these controls are pervasive; instead, management needs to address specifics relative to risk to the financial statements. For example, if there are problems hiring trained accounting staff, what processes and controls are involved, and are there sufficient management-level reviews and controls that would detect or prevent errors?

2. **Are there compensating or mitigating controls (they must be key controls that have tested effective)?** To what extent do they reduce the risk? If the answer is that the risk is fully addressed, the process can stop and the deficiency can be assessed as neither significant nor material. Management should further reassess whether this should remain a key control, as it may be redundant.

   IT general controls and entity-level controls again require special attention. Compensating and mitigating controls for ITGC issues may be found not only within ITGC, but within the business controls. For example, if developers are found to have access to production data, there is a risk that they could change the data (deliberately or inadvertently) and introduce errors into the financials. However, reconciliations and other business controls may be effective in promptly identifying such errors. Similarly, once the true risk presented by entity-level controls is identified, compensating controls may be found within the business processes.

3. **Is the potential error in the financials more than inconsequential?** If the assessment is that the error cannot be more than inconsequential (this may be 20 percent of the materiality level), then the process can be stopped. Management should confirm that this remains a key control.

   The assessment of whether the error could be more than inconsequential must consider where the error would occur in the financial statements. It is relatively straightforward when the error is in the P&L. However, if the effect is only on balance sheet accounts, the error should be considered using a materiality gauge related to that account, rather than the traditional P&L measure. For example, if there is a risk that fixed asset additions are not promptly recorded, the impact may be on understated depreciation, fixed assets, and accounts payable. Assume the following set of facts: materiality is set (based on P&L) at $10 million, the potential understatement of gross fixed assets and accounts payable is $6 million, and depreciation could be $150,000 understated. Total fixed assets are $500 million and accounts payable is $300 million. Management would assess the error separately in light of its effect on P&L, fixed assets, and accounts payable. It would conclude that the potential error is inconsequential, even though the total risk, at $6 million, appears at first glance to be high. This is because the error is small relative to the size of the balance sheet accounts.

   If the error would affect a disclosure, management needs to consider whether the error is material relative to the disclosed amounts and the significance to the investors (and potentially the regulators) of the specific disclosure. One measure that might be considered is whether the identification of an error of such an amount in a prior period's financial statements would result in needing to restate those financials.

4. **Is the risk of an error that is more than inconsequential more than remote?** Once it has been established that there is a risk of an error that is more than inconsequential, management must determine whether it meets the criteria for either a significant deficiency or a material weakness:

   a. Question 3 (above) identified that there is a possibility of an error that is more than inconsequential. The next step is to determine whether the likelihood of that happening is more than remote. As previously stated, "more than remote" means at least reasonably likely and is generally considered to be in the 5 percent to 10 percent range. If not, the process can stop. If there is such a risk, then the issue probably represents at least a significant deficiency.

   b. Is the risk of a material error more than remote? If not, then subject to question 5 (below), the issue is a significant, but not a material, weakness. However, if the risk of a material error is more than remote, then there is probably a material weakness.

5. **Would a reasonable individual assess the deficiency as material?** This is the key "acid" test. Given that management may not assess its system of internal control over financial reporting as effective once they identify a material weakness, they should ask some additional questions to validate the assessment of a deficiency as material.

a. Does management truly believe, and would a reasonable person concur, that the probability of a material error in future financial statements, which would not be detected by other controls, is in the 5 percent to 10 percent range or more? The PCAOB, in their Nov. 30, 2005 report, stated:

"The definitions in the standard [AS 2] … are designed to lead to a determination as to whether the deficiency would prevent a prudent official from concluding that he or she has reasonable assurance that transactions are recorded as necessary to permit the preparation of financial statements in conformity with generally accepted accounting principles.

"Further, the terms 'probable,' 'reasonably possible,' and 'remote,' should not be understood to provide for specific quantitative thresholds. Proper application of these terms involves a qualitative assessment of probability. Therefore, the evaluation of whether a control deficiency presents a 'more than remote' likelihood of misstatement can be made without quantifying the probability of occurrence as a specific percentage."

KEY POINTS

MATERIAL DEFICIENCIES

Does management truly believe, and would a reasonable person concur, that the probability of a material error in future financial statements, which would not be detected by other controls, is in the 5 percent to 10 percent range or more?

Would the deficiency prevent a prudent official from concluding that he or she has reasonable assurance that transactions are recorded as necessary to permit the preparation of financial statements in conformity with generally accepted accounting principles.

b. If the assessment of a deficiency is based on prior period errors, perhaps resulting in the restatement of prior period financials, is it reasonable to assess the current condition of internal controls (and therefore identify a material weakness) as ineffective?

This issue (assessing controls following a restatement) has become topical. While some external auditors have taken the position that there must be a material weakness if the financials are being restated, that is neither the position of the SEC nor the PCAOB. Both have indicated that while there is at least a significant deficiency, the underlying facts and circumstances must be considered. For example, if controls are improved in the current period by the hiring of additional technical accountants who then identify prior period accounting errors, then the current condition of internal controls is sound. The material weakness was in the prior and not the current period. On the other hand, if the error was detected by the external auditor and should have been, but was not, detected internally, that may indicate a material weakness in the technical competence of the internal staff.

H. ASSESSING THE ADEQUACY OF CONTROLS, INCLUDING ASSESSING DEFICIENCIES

To quote from the November 2005 PCAOB report: "Auditing Standard No. 2 describes certain circumstances that should be regarded as at least significant deficiencies and as strong indicators of a material weakness in internal control. The identification of one of these strong indicators is the beginning of the auditor's evaluation process of whether a material weakness, in fact, exists. Such indicators require heightened scrutiny, but they are not automatically material weaknesses. The Board's inspectors found that, in general, with respect to evaluating strong indicators — such as restatements of previously issued financial statements — auditors understood that the indicator required heightened scrutiny but was not irrefutable evidence of a material weakness."

Significant deficiencies need to be reported to the audit committee, and management is not required to disclose them in either the quarterly or annual reports filed with the SEC. Management should give strong consideration to sharing with the audit committee any issues that are borderline significant deficiencies, even though finally not assessed as such, as this is prudent communications. The remediation of a significant deficiency is probably[xxxv] a material change in the system of internal control and should be reported in the interim period within which it occurs.

Material deficiencies need to be considered and will affect both the quarterly Section 302 certification and the annual Section 404 assessment, if they are not corrected prior to year-end. Because the Section 404 assessment is as of year-end, management has the opportunity to achieve a "clean" opinion if they can identify the deficiency early, implement corrective actions, and then test the corrected operations prior to year-end. The external auditor will also need to test the operation of the remediated controls.

I. MANAGEMENT'S REPORT ON INTERNAL CONTROLS: THE END PRODUCT

Whether in the annual assessment for Section 404 or the quarterly certification for Section 302, the language of management's report will be based substantially on the advice of counsel. However, there are certain drivers that management should consider:

- Management has a great deal of latitude in describing the condition of its internal controls. The only formal requirement is that they don't assess the controls as effective when there is a material weakness. Other requirements are being defined over time as the SEC responds to filings and sets expectations for content (counsel can advise on these matters).
- The assessment should clearly describe management's opinion. What is the true condition of the system of internal control at the end of the year? Is it sufficiently robust to provide reasonable assurance that material errors will either be prevented or detected? The investor should be able to read the assessment and understand whether the company has adequate controls to run the business and report the results. (This is especially true when there is pressure to report a material weakness as a result of accounting errors in a prior period. Management should determine whether the current system of internal control is adequate, providing reasonable comfort related to the reliability of future financial statements, and not report deficiencies they do not believe relate to the current condition or future filings. In these circumstances, management may feel pressure to follow the rules at the expense of the principles. The assessment should reflect management's assessment of the controls and not mislead the investor as to their effectiveness.)
- The root cause of deficiencies should be understood. Control failures may be symptoms of a larger problem related to resources or management. The overall system will not be corrected until the larger problem is resolved, and, when known, the root cause should be reported. That is the true deficiency.
- When deficiencies are reported, sufficient related information should be provided to enable the investor to understand their significance, the risk they represent, and how management will ensure the integrity of future financial statements.

KEY POINTS

THE END PRODUCT

Management has a great deal of latitude in describing the condition of its internal controls. The only formal requirement is that they don't assess the controls as effective when there is a material weakness.

The assessment should clearly describe management's opinion. What is the true condition of the system of internal control at the end of the year? Is it sufficiently robust to provide reasonable assurance that material errors will either be prevented or detected? The investor should be able to read the assessment and understand whether the company has adequate controls to run the business and report the results.

J. CLOSING THOUGHTS ON EFFICIENCY

All agree that the Section 404 requirement has improved the quality of internal control systems through increased attention by both management and the external auditor. However, there is less than universal agreement that the improvement has been justified relative to the enormous cost.

> *KEY POINT*
>
> **EFFICIENCY**
>
> *Is the Section 404 program itself assessed for effectiveness on a continuing basis, to ensure it is improved as the organization learns from experience and benefits from changes in regulations or their interpretation?*

The following checklist may help management teams ensure their Section 404 program is efficient.

1. Has operating management taken ownership of their processes and documentation, rather than leaving it to the Section 404 team or the internal audit function?

2. Does operating management update all process and control documentation promptly throughout the year and not just when testing starts? Is there an effective change management process in place, including the timely assessment of process changes for their potential impact on key controls?

3. Is operating management committed to prompt assessment and remediation of all control deficiencies? Where not justified based on management's assessment of risk and cost, is management committed to providing such assessment promptly so the effect on management's overall assessment of controls can be identified and discussed with senior management?

4. Has a top-down, risk-based approach been used to identify the key controls? Is management confident that all identified key controls are truly key? Has the design of the related processes been reviewed to determine if changes can result in fewer and more effective controls, relying more on automated controls or on higher-level controls (e.g., detailed reconciliations and flux analyses)? The fewer the controls to test, the lower the cost.

5. Is management of the Section 404 program at a sufficiently high level within the organization to:
   - Influence operating management relative to completion of their responsibilities?
   - Communicate effectively with executive management relative to progress and potential issues?
   - Negotiate as needed with the external auditor (e.g., to increase reliance on management testing, agree on key controls early, or address concerns as they arise)?

6. Is the use of internal resources optimized, including the use of internal auditors to perform testing or to validate testing performed by management staff?

7. Has overall staffing been optimized, reducing reliance on more expensive external consultants and testers?

8. Has reliance by the external auditor on management testing been optimized?

J. CLOSING THOUGHTS ON EFFICIENCY

9. Does the external auditor follow a top-down, risk-based approach as discussed in the May 16 and Nov. 30, 2005, PCAOB documents?

10. Is there a detailed project plan:
    - That includes a walkthrough of all significant processes early in the year (preferably in the first quarter)?
    - With testing scheduled in such a way that all key controls are tested by mid-year, with additional testing to update the results scheduled closer to year-end? This enables the external auditors to start their walkthroughs and testing early, providing time for management to address and remediate any deficiencies identified in either management or external auditor testing.
    - That includes all key activities required to complete the program, including fraud risk assessment, end-user computing issues, assessment of SAS 70 reports from service providers, etc.?
    - That details all required resources, including specialists (e.g., for IT and/or tax processes and controls), so they can be scheduled early?
    - With regular reporting to senior management that focuses on key metrics and issues, such as:
      - Progress against an established timetable, highlighting steps that are or may be behind schedule?
      - The percentage of key controls tested compared to scheduled completion level?
      - The number and percentage of key controls failing?
      - The number of failed controls that are potentially significant to the Section 404 assessment?
      - The number of failed controls where remediation will not be completed within 30 days (so senior management can focus on timely completion)?
      - The number of key controls where remediation and retesting may not be completed with sufficient time for the external auditor to retest (these are likely to be open deficiencies at year-end)?
      - Costs to date and projected through the end of the year?
      - Potential resource issues?
      - Other issues, such as coordination and concerns raised by the external auditor?

11. Has there been communication and coordination with all service providers to ensure that a SAS 70 type II report will be available at the appropriate time, and that early warning of potential deficiencies identified during the SAS 70 audit is provided?

12. Finally, is the Section 404 program itself assessed for effectiveness on a continuing basis, to ensure it is improved as the organization learns from experience and benefits from changes in regulations or their interpretation?

ADDITIONAL REFERENCE MATERIALS

SEC:

- "Final Rule: Management's Reports on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports" at http://www.sec.gov/rules/final/33-8238.htm

- "Commission Statement on Implementation of Internal Control Reporting Requirements" (May 16, 2005) at http://www.sec.gov/news/press/2005-74.htm

- "Management's Report on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports - Frequently Asked Questions" (revised Oct. 6, 2004) at http://www.sec.gov/info/accountants/controlfaq1004.htm

PCAOB:

- "Auditing Standard No. 2: An Audit of Internal Control Over Financial Reporting Performed in Conjunction With an Audit of Financial Statements" at http://www.pcaobus.org/Rules/Rules_of_the_Board/Auditing_Standard_2.pdf

- "Policy Statement Regarding Implementation of Auditing Standard No. 2" (May 16, 2005 guidance) at http://www.pcaobus.org/Rules/Docket_014/2004-09-15_Release_2004-008.pdf

- "Staff Questions and Answers on Auditing Standard No. 2" at http://www.pcaobus.org/Standards/Staff_Questions_and_Answers

- "Report On The Initial Implementation Of Auditing Standard No. 2, An Audit Of Internal Control Over Financial Reporting Performed In Conjunction With An Audit Of Financial Statements" at http://www.pcaobus.org/Rules/Docket_014/2005-11-30_Release_2005-023.pdf

COSO:

- "Internal Control — Integrated Framework, Executive Summary" at http://www.coso.org/publications/executive_summary_integrated_framework.htm

THE IIA:

- "Internal Auditing's Role in Sections 302 and 404 of the Sarbanes-Oxley Act" at http://www.theiia.org/download.cfm?file=1655

- "Sarbanes-Oxley Section 404 Work: Looking at the Benefits" at http://www.theiia.org/?doc_id=5161

DELOITTE:

- "Taking Control: A Guide to Compliance with Section 404 of the Sarbanes-Oxley Act of 2002" at http://www.deloitte.com/dtt/whitepaper/0,1017,sid%253D36513%2526cid%253D54135,00.html

- "Sarbanes-Oxley Section 404: 10 Threats to Compliance" at http://www.deloitte.com/dtt/article/0,1002,sid%253D36513%2526cid%253D58359,00.html

ADDITIONAL REFERENCE MATERIALS

ERNST & YOUNG:

- "Emerging Trends in Internal Controls — Third Survey" at http://www.ey.com/global/content.nsf/US/AABS_-_Assurance_-_Library_-_Registration

- E&Y Summary – PCAOB Standard No. 2: Audits of Internal Control Over Financial Reporting at http://www.ey.com/global/content.nsf/US/AABS_-_Assurance_-_Library_-_Registration

KPMG:

- "Making Sarbanes-Oxley Section 404 Compliance Sustainable" at http://www.us.kpmg.com/RutUS_prod/Documents/9/Sustaining_Web.pdf

PRICEWATERHOUSECOOPERS:

- "Management's Responsibility for Assessing Internal Control Effectiveness of Financial Reporting Under Section 404 of the Sarbanes-Oxley Act" at http://www.pwc.com/extweb/pwcpublications.nsf/4bd5f76b48e282738525662b00739e22/75d798ef7d9fc9c385256e3e005cec14

- "How to move your company to sustainable Sarbanes-Oxley compliance — from project to process" at http://www.pwc.com/Extweb/pwcpublications.nsf/docid/31F021B50359960385256FF60056C4B6/

PROTIVITI:

- "Guide to the Sarbanes-Oxley Act: Internal Control Reporting Requirements - Third Edition" at http://www.protiviti.com/?pgTitle=Sarbanes-Oxley%20Section%20404%20FAQs

FINANCIAL EXECUTIVES INTERNATIONAL:

- "Sarbanes-Oxley Section 404 Implementation Survey" at http://www.fei.org/404_survey_3_21_05.cfm

- "Sarbanes-Oxley Section 404 Compliance: From Project to Sustainability"

NOTES

i See the Additional Reference Materials section for links to the major sites.

ii Included in the quarterly financial statements filed on Form 10-Q with the SEC.

iii "Report On The Initial Implementation Of Auditing Standard No. 2, An Audit Of Internal Control Over Financial Reporting Performed In Conjunction With An Audit Of Financial Statements," PCAOB Release No. 2005-023, Nov. 30, 2005.

iv Of note is this excerpt from Institutional Shareholder Services' "ISS U.S. Corporate Governance Policy - 2006 Updates":

> "Companies with significant material weaknesses identified in the Section 404 disclosures potentially have ineffective internal financial reporting controls, which may lead to inaccurate financial statements, hampering shareholders' ability to make informed investment decisions, and may lead to the destruction of public confidence and shareholder value."

v Executives at some companies have informed the authors that their external auditors told them if they have more than a specified number of control deficiencies, they could not assess their controls as effective. Others have been told that specific deficiencies (for example, failing to monitor the activities of the database administrator, or failing to have a comprehensive fraud assessment program) are always at least significant and probably material deficiencies. These specific cases are not consistent with the language (and we believe the intent) of AS 2, nor of the guidance from the SEC. Although some may disagree, AS 2 is fundamentally a principles-based standard that emphasizes the use of judgment by both management and the external auditor.

vi In this guide, the terms *material error* and *material misstatement* have been used inter changeably to represent the risk of a material error in the financial statements filed with the SEC, regardless of whether the error is the result of fraud or an inadvertent control failure.

vii In AS 2, the PCAOB used the term "reasonably possible." In developing the rules for the Section 404 report, the SEC used the term "reasonably likely." In this guide, we have used the terms synonymously, meaning more than remote, but less than probable.

viii The user of the Section 404 assessment should understand that the quality of the system of internal control as of the reporting date is only an indication of future results and depends, among other matters, on there being no significant change to the internal control financial report (ICFR). It should be noted that the PCAOB requires (in AS 2) that the report of the external auditors include the following statement: "projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions, or that the degree of compliance with the policies or procedures may deteriorate."

ix The Financial Executives International (FEI) study released in May 2005 reports external costs represented approximately 57 percent of total costs.

x Surveys on external audit costs related to Section 404 have varied significantly. Although some have indicated an average increase of 40 percent (the FEI study released in May 2005 reports the portion of the auditors' fees related to Section 404 averaged 57 percent of the annual statement fee), many companies have experienced far greater increases. A December 2005 survey by CRA International reported that external auditor costs represented only 26 percent of total Section 404 costs at larger companies, with market capitalization more than $700 million, and 25 percent at smaller companies. By contrast, the FEI study shows external auditor fees averaged about 43 percent of total costs.

xi The role of the internal audit function in Section 404 testing has been discussed in detail in The IIA's report "Internal Auditing's Role in Sections 302 and 404 of the Sarbanes-Oxley Act," released on May 26, 2004. Key points addressed in the document related to assistance with testing include:

> "It is management's responsibility to ensure the organization is in compliance with the requirements of Sections 302 and 404 and other requirements of the Act, and this responsibility cannot be delegated or abdicated. Support for management in the discharge of these responsibilities is a legitimate role for internal auditors. The internal auditors' role in their organization's Sarbanes-Oxley project can be significant, but also must be compatible with the overall mission and charter of the internal audit function. Regardless of the level and type of involvement selected, it should not impair the objectivity and capabilities of the internal audit function for covering the major risk areas of their organization. Internal auditors are frequently pressured to be extensively involved in the full compendium of Sarbanes-Oxley project efforts as the work is within the natural domain of expertise of internal auditing." (Executive Summary)

> "Activities that are included in the internal auditor's recommended role in supporting the organization in meeting the requirements of Sections 302 and 404 include:
> - Project Oversight.
> - Consulting and Project Support.
> - Ongoing Monitoring and Testing.
> - Project Audit."
>
> (Recommended Role of Internal Audit)

> "Ongoing Monitoring and Testing
> - Advise management regarding the design, scope, and frequency of tests to be performed.
> - Independent assessor of management testing and assessment processes.
> - Perform tests of management's basis for assertions.
> - Perform effectiveness testing (for highest reliance by external auditors).
> - Aid in identifying control gaps and review management plans for correcting control gaps.
> - Perform follow-up reviews to ascertain whether control gaps have been adequately addressed.

- Act as coordinator between management and the external auditor as to discussions of scope and testing plans.
- Participate in disclosure committee to ensure that results of ongoing internal audit activities and other examination activities, such as external regulatory examinations, are brought to the committee for disclosure consideration."

(Recommended Role of Internal Audit)

xii In some cases, efficiencies can also be achieved through a redesign of the controls. Some believe that reliance on more automated controls may allow a reduction of cost, as automated controls need to be tested only once, while manual control testing generally requires a larger sample of transactions. However, increasing the number of automated controls may also require additional testing of IT general controls, which is relatively expensive. Any redesign to achieve cost-savings in testing should consider the total cost of testing, including testing of IT general controls.

xiii The SEC provided guidance, in its January 2002 Frequently Asked Questions (FAQ) No. 22, that a formal evaluation of internal controls (similar to that required for Section 404) is not required by current regulations to complete the Section 302 certification. Their answer to FAQ 22 is excerpted in note xxxv below.

xiv Small businesses and foreign filers will use the equivalent forms: 10KSB and 20-F.

xv It is notable that the Foreign Corrupt Practices Act of 1977 directed that internal controls are the responsibility of management.

xv[i] PCAOB AS 2 is based on the COSO definition of internal control, as is Codification of Statements on Auditing Standards Section 319 ('Auditing Standards Section 319).

xvii Securities Exchange Act Rules 13a-15(f) and 15d-15(f).

xviii COBIT 4.0 is available at www.isaca.org/cobit.

xix This is described further in "A Framework for Internal Auditing's Entity-Wide Opinion on Internal Control" (IIA Research Foundation, 2004) and "Internal Audit Reporting Relationships: Serving Two Masters" (IIA Research Foundation, 2003).

xx The rules were first mentioned in an SEC release in August 2002 and incorporated into the Securities Exchange Act of 1934 (as amended) Rules 13a-15(e) and 15d-15(e).

xxi In question 23 of its October 2004 FAQ report, the SEC addressed whether the assessment of internal controls over financial reporting included required supplementary schedules. As indicated below, their conclusion was that the assessment does not currently need to be included within the scope of that assessment.

"Q: The Commission's rules implementing Section 404, announced in Release No. 34-47986, require management to perform an assessment of internal control over financial reporting which includes the 'preparation of financial statements for external purposes in accordance with generally accepted accounting principles.' Does management's assessment under the Commission's rule specifically require management to assess internal control over financial reporting of required supplementary information? Supplementary information includes the financial statement schedules required by Regulation S-X as well as any supplementary disclosures required by the Financial Accounting Standards Board (FASB). One of the most common examples of such supplementary information is certain disclosures required by the FASB Standard No. 69, Disclosures about Oil and Gas Producing Activities.

"A: Adequate internal controls over the preparation of supplementary information are required and therefore should be in place and assessed regularly by management. The Commission's rules in Release No. 34-47986 did not specifically address whether the supplementary information should be included in management's assessment of internal control over financial reporting under Section 404. A question has been raised as to whether the supplementary information included in the financial statements should be encompassed in the scope of management's report on their assessment of internal control over financial reporting.

"The Commission staff is considering this question for possible rulemaking. Additionally, the Commission staff is evaluating broader issues relating to oil and gas disclosures and will include in its evaluation whether rulemaking in this area may be appropriate. Should there be any proposed changes to the current requirements in this area, they will be subject to the Commission's standard rulemaking procedures, including a public notice and comment period in advance of rulemaking. As a result, internal control over the preparation of this supplementary information need not be encompassed in management's assessment of internal control over financial reporting until such time that the Commission has completed its evaluation of this area and issues new rules addressing such requirements."

xxii Current reports include Form 6-K, definitive proxy materials, and definitive information statements.

xxiii In its final rules implementing Section 404, the SEC made the following comments related to the difference between internal controls over financial reporting and disclosure controls. Please note the italicized sections:

"We agree that some components of internal control over financial reporting will be included in disclosure controls and procedures for all companies. *In particular, disclosure controls and procedures will include those components of internal control over financial reporting that provide reasonable assurances that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles.* However, in designing their disclosure controls and procedures, companies can be expected to make judgments regarding the processes on which they will rely to meet applicable requirements. In doing so, *some companies might design their disclosure controls and procedures so that certain components of internal control over financial reporting, pertaining to the accurate recording of transactions* *and disposition of assets, or to the safeguarding of assets, are not included*. For example, a company might have developed internal control over financial reporting that includes as a component of safeguarding of assets dual signature requirements or limitations on signature authority on checks. That company could nonetheless determine that this component is not part of disclosure controls and procedures. *We therefore believe that while there is substantial overlap between internal control over financial reporting and disclosure controls and procedures, many companies will design their disclosure controls and procedures so that they do not include all components of internal control over financial reporting."*

We concur with the SEC's observation that the referenced controls could be part of a company's system of internal control and yet not be included in disclosure controls. However:

- As noted by the SEC, disclosure controls will include all the components of internal control over financial reporting required to provide reasonable assurance over the reliability of the financial statements. By definition, those are key controls.
- The controls that the SEC has referenced as examples of controls that are included in ICFR but excluded from disclosure controls would not be considered key controls for Section 404 purposes.

Therefore, although the SEC's position is that there is only "substantial overlap" between ICFR and disclosure controls, in practice, the authors believe there will be few situations where key controls for Section 404 are not included in disclosure controls.

Some experts, including certain specialized attorneys, have taken a different approach. Arguments include:

- Disclosure controls only relate to the design of controls and not their operation. If a material weakness relates only to the operation of a control (i.e., it is adequately designed but not consistently followed), these experts believe management can report an ineffective system of internal control for Section 404, but an effective system of disclosure controls for Section 302. However, the authors believe such a determination is likely to confuse, rather than inform investors.
- Safeguarding of assets is included in the scope of internal controls for Section 404 but not in disclosure controls for Section 302. However, ICFR for Section 404 relates to controls that prevent or detect a misstatement of the financials. A misstatement of the financials filed with the SEC is, by definition, within the scope of disclosure controls.

xxiv In this guide, the term *interim assessment* of internal controls or disclosure controls is used to refer to what the SEC describes as the *periodic evaluation* of those controls.

xxv Some companies and external auditors have considered materiality relative to interim financial statements when defining significant accounts. In their May 2005 Staff Report, the SEC made it very clear that:

> "Companies generally should determine the accounts included within their Section 404 assessment by focusing on annual and company measures rather than interim or segment measures. If management identifies a deficiency when it tests a control, however, at that point it must measure the significance of the deficiency by using both quarterly and annual measures, also considering segment measures where applicable."

xxvi The SEC and PCAOB guidance references "significant accounts," meaning individual lines in the financial statements, rather than "significant *general ledger* accounts." We recommend defining significant accounts at the general ledger level, as this provides an improved opportunity to refine the scope of the Section 404 assessment. For example, an individual line in the financial statements may be below the planning materiality level — but contain a number of general ledger accounts that exceed planning materiality and that may not always offset each other.

Management may, for a number of reasons, find that some individual lines in the financial statements do not appear to have any significant general ledger accounts. For example, the numbers may be small. In this case, at least one key control must be identified — as each line is presumed to be significant. Management should consider whether there is one or more higher level controls that provide the necessary assurance that any material error in the line would either be prevented or detected.

xxvii The timely detection of an error is critical, otherwise detection may occur after the financial statements have been filed with the SEC, leading to the potential need for restatement.

xxviii It is possible for the external auditor and management to take top-down and risk-based approaches and reach different conclusions on which controls are key. As long as management has followed a reasonable process and defined key controls that address the likely risks to significant accounts, the external auditor should be able to draw a satisfactory opinion with regard to management's assessment.

xxix The PCAOB discussed benchmarking (Staff Questions and Answers, May 16, 2005, Number 45) as follows :

> "In general, to render an opinion as of the date of management's assessment, the auditor needs to test controls every year. This type of evidence is needed regardless of whether controls were found to be effective at the time of the prior annual assessments or whether those controls have changed since that time, because even if nothing significant changed about the company — the business model, employees, organizational structure, etc. — controls that were effective last year may not be effective this year due to error, complacency, distraction, and other human conditions that result in the inherent limitations in internal control over financial reporting. Automated application controls, however, will continue to perform

a given control (for example, aging of accounts receivable, extending prices on invoices, performing edit checks) in exactly the same manner until the program is changed. Entirely automated application controls, therefore, are generally not subject to breakdowns due to human failure, and this feature allows the auditor to 'benchmark,' or 'baseline,' these controls.

"If general controls over program changes, access to programs, and computer operations are effective and continue to be tested, and if the auditor verifies that the automated application control has not changed since the auditor last tested the application control, the auditor may conclude that the automated application control continues to be effective without repeating the prior year's specific tests of the operation of the automated application control. The nature and extent of the evidence that the auditor should obtain to verify that the control has not changed may vary depending on the circumstances, including depending on the strength of the company's program change controls.

"When using a benchmarking strategy for a particular control, the auditor also should consider the importance of the effect of related files, tables, data, and parameters on the consistent and effective functioning of the automated application control. For example, an automated application for calculating interest income might be dependent on the continued integrity of a rate table used by the automated calculation.

"To determine whether to use a benchmarking strategy, the auditor should evaluate the following factors. As these factors increase in significance, the control being evaluated should be viewed as well suited for benchmarking. As these factors decrease in significance, the control being evaluated should be viewed as less suited for benchmarking. These factors are:

- The extent to which the application control can be matched to a defined program within an application.
- The extent to which the application is stable (i.e., there are few changes from period to period); and whether a report of the compilation dates of all programs placed in production is available and is reliable. (This information may be used as evidence that controls within the program have not changed.)

"Benchmarking automated application controls can be especially effective for companies using purchased software when the possibility of program changes is remote — for example, when the vendor does not allow access or modification to the source code.

"At some point, the benchmark of an automated application control should be reestablished. To determine whether to reestablish a benchmark, the auditor should evaluate the following factors:

- The effectiveness of the IT control environment, including controls over application and system software acquisition and maintenance, access controls, and computer operations.

- The auditor's understanding of the effects of changes, if any, on the specific programs that contain the controls.
- The nature and timing of other related tests.
- The consequences of errors."

xxx Management can reference the PCAOB's answer to Question 24 on Service Organizations in its "Staff Questions and Answers" issued June 23, 2004.

xxxi Paragraph 24 of Auditing Standard No. 2

xxxii SAS 99 makes a similar statement: "For purposes of the Statement, fraud is an intentional act that results in a material misstatement in financial statements that are the subject of an audit."

xxxiii This was affirmed in the PCAOB guidance to the CPA firms on May 16, 2005, in Staff Questions and Answers, Number 47 and Number 49. The relevant passages are in italics.

47: *Management's daily interaction with the system of internal control provides it with a broader array of procedures to achieve reasonable assurance for its assessment of internal control over financial reporting than the auditor has available.* The auditor should recognize this difference when evaluating the adequacy of management's assessment.

"Paragraph 40 of Auditing Standard No. 2, which addresses the auditor's evaluation of management's assessment process, recognizes the important difference between management's assessment and the auditor's testing. The fifth bullet of that paragraph cites as *examples of procedures that management could use to obtain sufficient evidence of the operating effectiveness of controls 'inspection of evidence of the application of controls, or testing by means of a self-assessment process, some of which might occur as part of management's ongoing monitoring activities.' For example, management might be able to determine that controls operate effectively through its direct and ongoing monitoring of the operation of controls.* This determination might be accomplished through performing regular management and supervisory activities, monitoring adherence to policies and procedures, and performing other routine actions. For instance, a supervisor's review of a monthly account reconciliation prepared by one of his or her subordinates could be a monitoring control that also provides management with evidence supporting its assessment of internal control over financial reporting, if the results of the supervisor's review were evaluated and documented as part of management's assessment. To appropriately evaluate the adequacy of management's assessment as directed by the standard, the auditor needs to recognize these other types of procedures that are available to management as part of the basis for its assessment.

"**49:** *The auditor should not evaluate the adequacy of management's assessment by simply comparing, on a control-by-control level, whether management's testing was at least as extensive as the auditor's. The nature and extent of the procedures* *that management uses to support its assessment should be determined by management, independent of the auditor's decisions about the nature, timing, and extent of the auditor's procedures. The procedures that management performs to support its assessment might be different from the auditor's procedures, yet still provide management with an adequate basis for its assessment, for several reasons.*

"First, as discussed in Staff Question No. 47, *management has a broader array of procedures available to support its assessment than the auditor. As discussed further in Staff Question No. 48, management also may use self-assessment in particular areas to support its overall assessment of internal control over financial reporting. In this circumstance, the auditor should evaluate whether management's overall assessment process includes periodic, objective validation of the effectiveness of self- assessments in individual areas, such as testing by internal auditors, to verify the effectiveness of self-assessments. This type of validation of self-assessments need not occur every period for every area in which a self-assessment is performed. Management's overall assessment process, however, should include a rational approach for determining how frequently and extensively to verify the effectiveness of self-assessments.*

"The work that management performs in connection with its assessment can have a significant effect on the nature, timing, and extent of the work of the auditor. The more extensive and reliable management's assessment is, the less extensive and costly the auditor's work will need to be."

xxxiv Some companies have gained efficiencies by conducting joint walkthroughs with the external auditors (this is more likely when the management testing is performed by the internal audit function).

xxxv The framework was developed by nine CPA firms in association with a respected academic. It can be found at the Financial Executives International's (FEI's) Web site: http://www.fei.org/download/Framework_10_29.pdf#search='Process%2FTransactionLevel%20Exceptions%20and%20Deficiencies

xxxvi We recommend consulting with SEC counsel, although it appears reasonable to assume that if a material weakness is material to the investor, then its resolution is highly likely to be a material change in the system of internal controls — and similarly likely to be material to the investor.

In January 2002, SEC staff issued answers to a number of FAQ. The answer to question 22 is relevant, and key portions are highlighted in the extract below:

"Although proposed amendments to Exchange Act Rules 13a-15 and 15d-15 would impose a requirement on an issuer's management to conduct an evaluation, with the participation of the issuer's CEO and CFO, of the effectiveness of the issuer's internal controls and procedures for financial reporting … the Commission's rules currently do not specifically require an issuer's CEO or CFO, or the issuer itself, to conduct periodic evaluations of the issuer's internal controls or the issuer's internal controls and procedures for financial reporting. Some elements of internal controls are included in the definition of *disclosure controls and procedures*. There is a current evaluation requirement involving the CEO and the CFO of that portion of internal controls that is included within disclosure controls and procedures as part of the required evaluation of disclosure controls and procedures. We expect that issuers generally also would engage in an evaluation of internal controls. We believe that issuers generally currently evaluate internal controls, for example, in connection with reviewing compliance with Section 13(b) of the Exchange Act or in connection with the preparation or audit of financial statements.

"[T]o the extent that an issuer has conducted an evaluation of its internal controls as of the end of the period covered by the report, including under the circumstances described

in the preceding paragraph, *the issuer should disclose any significant changes to the internal controls* or in other factors that could significantly affect these controls subsequent to the date of their evaluation, *including any corrective actions with regard to significant deficiencies and material weaknesses.* If the issuer has made any significant changes to internal controls or in other factors that could significantly affect these controls, such changes would presumably follow some evaluation, in which case the required disclosure must be made."

ACKNOWLEDGEMENTS

The Institute of Internal Auditors would like to thank several individuals who assisted in developing this guide. The principal author was Norman Marks. Contributions were made by Philip Moulton and Pierre Pradal. We would also like to thank the following for taking the time to review drafts and provide constructive suggestions for improvement:

Bruce Adamec

Dick Anderson

Doug Anderson

Hubertus Buderath

Jackie Cain

Lee Ann Campbell

Roger Herd

Steve Jameson

Tim Leech

Sandford Liebesman, Ph.D.

Warren Malmquist

Patricia Miller

Heriot Prentice

Larry Rittenberg, Ph.D.

Peter Schlesiona

Kyoko Shimizu

Gil Simonetti

Dan Swanson

James M. Sylph

Jay Taylor

Jeffrey Thomson

Louis Vaurs

Curt Verschoor, Ph. D.

Jody Whitley

The Institute of Internal Auditors

PROFESSIONAL GUIDANCE
Setting the Standard

Order No. 1014
Member US $25
Nonmember US $30
Event pricing US $ 22.50

ISBN 0-89413-593-7
52
9 788941 389378

THE INSTITUTE OF INTERNAL AUDITORS
Attachment C
Additional Issues of Interest to be Considered

The IIA's key issues that should be addressed prior to year 3 implementation were presented in the main body of our response. However, we have additional suggestions, grouped in the same categories, listed below. We believe these changes will further improve the §404 process and recommend that the SEC and PCAOB address these as priorities permit.

I. Additional Guidance Needed for Both Management and Audit Firms

A. We believe improved guidance related to obtaining a high level of assurance is needed. The lack of detailed guidance by the SEC to management on what is expected of them regarding the control assessment process has caused management in many cases to turn to their external auditors to obtain guidance on what is acceptable. This has resulted in the PCAOB setting the standard for management on what is required to perform a control assessment rather than management setting the standard based on the guidance from the SEC.

Areas of potential guidance should include integration of SAS 99 and §404 work related to fraud, scoping of Information Technology General Controls (ITGC), and definitions like "remote likelihood," "reasonably possible," and "reasonable assurance." The topic of "reasonable assurance" continues to be problematic. Unfortunately, the clarification that reasonable assurance represents a high level of assurance is not particularly useful because systems of internal control are not perfect. They will fail, even if infrequently, and when they do, that does not necessarily indicate a control deficiency – even if a material error results.

The guidance discusses likelihood (e.g., "more than remote likelihood" or "at least reasonably possible") without the context of a timeframe. Without a defined timeframe, all potential risks are highly likely to occur. Further, when assessing the quality of the system of internal control over financial reporting (ICFR) at a company, the value to the investor is the assurance that ICFR is of a sufficient quality to provide reasonable assurance that material error in *future* filings' financial statements will either be prevented or detected. The financial statements with which the assessments by management and the external auditor are filed have been audited and both have attested to them. We believe it is reasonable to use a measurement of the quality of ICFR as whether it provides a reasonable level of assurance relative to material errors in the next 12 months' filed financial statements.

B. A common definition of a key control is needed, as this is the core of the §404 testing. We suggest the definition included in the IIA publication, *Sarbanes-Oxley Section 404: A Guide for Management by Internal Control Practitioners* (Attachment B): "A key control is a control that, if it fails[i], 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[ii]. In other words, a key control is one that provides reasonable assurance that material errors will be prevented or timely detected."

C. The IIA believes the SEC and PCAOB should be aware that external auditors are in some cases applying poor judgment as outlined in this response. Registrants must settle disputes with their auditor in a timely manner due to deadlines for publishing financial statements. We are concerned that unless the issues in this response are addressed, audit firms may continue to hide behind a process designed by the SEC and PCAOB and continue to apply poor judgment. We believe that transparent guidance will go a long way to resolving many of these concerns.

D. Additional guidance regarding the quarterly §302 assessment process and the reporting on the status of remediation efforts to handle material weakness disclosures would be well received. When assessing changes in ICFR, what constitutes a major change in internal control and its performance (e.g., definition of a material change in internal control)? Also, a specific issue that needs to be addressed is when a material change in internal control is assumed to occur when it relates to implementation of new processes or systems over a period of multiple quarters.

II. Need for Increased Reliance on Work of Others

E. Audit firms should place increased reliance on the work of others to the extent possible related to their assessment of the control environment. Our survey results about the extent of the external auditor's reliance on the work of others, including the internal auditor's, shows progress, but with a need for improvement. We believe costs could be reduced further, without impacting the quality of compliance, by greater utilization of internal auditor work. Cost reduction, in the end, is one of the biggest, if not the primary, driver of sustainability.

The IIA believes an organization with an established internal audit function operating in full compliance with the *Standards* and The IIA's definition of internal auditing is already well equipped to meet the challenge of good governance and transparency of internal control effectiveness and efficiency. The *Standards* require the internal audit function to implement a quality assurance and improvement program and have an external quality assurance review a minimum of every five years.

AS 2 provides external auditors with specific guidance on when and how they can use the work of others in performing their audit of ICFR. The effectiveness and efficiency of an external auditor's testing of ICFR would be improved with the following changes:

1. Allow the external auditor to selectively rely on the work of others related to their assessment of the control environment

Paragraph 112 of AS 2 describes factors for external auditors to consider when determining the ability to rely on the work of others or to perform the work themselves. These factors include the degree of judgment required to evaluate the operating effectiveness of the controls, the level of judgment or estimation required, and the potential for management override. These factors are not reiterated in paragraph 113 where the external auditors are instructed that they can never rely on any work of others in relationship to the elements of the control environment, which has caused additional work. The guidance in paragraph 113 is only consistent with paragraph 112 if every aspect of the control environment is so highly judgmental that reliance on others is unacceptable, but this is not typically the case. For example, the following elements of an effective control environment are not highly judgmental and can be effectively assessed by others:

- Existence of a written code of conduct and consistency of this code with other formal and informal policies, practices and standards of the business
- Methods of interacting with suppliers, customers, creditors, etc. as evidenced by written agreements, policies, and standards
- Formal job descriptions that define tasks of particular jobs
- Frequency and timeliness of board of directors or audit committee meetings
- Sufficiency and timeliness with which the board of directors or audit committee is appraised of sensitive information, investigations, or improper acts
- Frequency of interactions between senior management and operating management
- Adequacy of definition of key manager's responsibilities
- Appropriateness of control-related standards and procedures, including job descriptions
- Extent to which policies and procedures for hiring, training, promoting, and compensating employees are in place
- Appropriateness of remedial action taken in response to departures from approved policies
- Adequacy of employee candidate background checks

In each of the above areas, the guidance of AS 2 has led external auditors to ignore information prepared and analyzed by others. The external auditors believe the guidance of paragraph 113 requires them to perform the entire data gathering, testing of the integrity of that data, and evaluation of the data themselves. For many of these areas, and for many aspects of the evaluation process, relying on the work of others (such as by a competent and independent internal audit function) would be more efficient and effective. The information does not require a high level of complex judgment to gather and evaluate, and the prohibition in paragraph 113 is overly restrictive.

2. Allow the external auditor to rely on the work of others for some walkthroughs

AS 2, paragraph 116, directs the external auditor to perform all walkthroughs themselves, regardless of the risk of the area being audited or the ability of others to adequately evaluate and document a walkthrough. A walkthrough can be an extremely useful mechanism for understanding a process and the related internal controls. However, the prohibition on the external auditor considering reliance on the work of others essentially implies that no one other than an external auditor can understand a process and document it through a walkthrough.

The principles behind the guidance in paragraph 126, the fifth bullet point, should be applied to reliance on the work of others for walkthroughs (i.e. there will be instances in which processes involve a low degree of judgment in evaluating operating effectiveness of controls, have a low potential for management override, and/or are simple in their construction). In such situations, the external auditor should be allowed to exercise judgment and elect to rely on the walkthrough work performed by others. The current prohibition in paragraph 113 is overly restrictive.

3. Provide additional guidance on how to determine principal evidence

AS 2, paragraph 108, provides some general guidance to the external auditor on how to determine whether their testing provides the principal evidence for their opinion. In practice, this guidance has proven to be inadequate, resulting in the external auditor relying on the work of others for much less than the guidance would suggest. The note at the end of paragraph 108 suggests that not all evidence is of the same importance in determining how much the principal evidence is. This nuance has been missed.

In practice, The IIA believes that even though external auditors are not placing appropriate reliance on the work of others for areas like entity-level controls and pervasive controls, they continue to operate in a manner that suggests they must also personally obtain the majority of the evidence related to all other controls, including low-risk, routine transactions.

The scandals that were a large part of the rationale behind the requirements of §404 dealt with management override of controls, highly subjective areas, and non-routine transactions. Focusing an external auditor's attention on these areas should provide a large degree of evidence in the areas of high risk. However, some external auditors continue to treat all individual elements of internal control equally and personally review the majority of the evidence for all elements of control individually, regardless of risk.

The guidance currently stated in AS 2 could be enhanced and more explicit guidance on the requirements for obtaining principal evidence is needed to allow a more effective and efficient approach to this work.

4. Modify guidance regarding extent of testing the work of others

AS 2 paragraphs 123 and 124 provide guidance regarding the external auditor testing some of the work of others. While paragraph 123 provides two alternative methods, experience has shown that external auditors prefer the first alternative (i.e., retest controls that others tested) over the second alternative (i.e., testing similar controls not actually tested by others). The result is frequent duplicative testing by both internal auditors and external auditors.

In addition, paragraph 124 seems to imply that only this testing by the external auditor provides information on the quality and effectiveness of the test work of others. When testing is performed by an internal audit function that complies with IIA *Standards*, the external auditor has additional methods to confirm quality and effectiveness. IIA *Standards* require periodic quality assurance reviews by third parties, on-going internal quality processes, adherence to established quality practices, and maintenance of a skilled and trained work force.

III. Continued Improvement in the Effectiveness and Efficiency of the §404 Process

F. The external auditor should be able to determine whether partial reliance on the results of testing from prior years is acceptable. Such reliance will more likely be possible when the design and operation of the controls has not changed significantly from the prior year and the risk of a control failure leading to a material error is relatively low.

Paragraph 105 requires the external auditor to design tests to provide a high level of assurance that the control being tested is operating effectively. The level of assurance required must correspond to the level of risk present in the control. While this concept is alluded to, in the third bullet under paragraph 105, it is not well developed. The following highlight the gaps in AS 2:

1. Audit results from testing in prior years should allow the external auditors to consider a shift in their testing. For example, during annual audits of controls of a transactional system, the external auditors may find that controls are well designed and expertly executed. The auditors should consider shifting their testing methods from detailed re-performance of transactions to identifying the key controls required to keep the risk of material misstatement to less than reasonably likely. The current guidance allows external auditors to vary the type and extent of testing based on risk, but experience has show that external auditors tend to focus more on the requirement that every year must stand on its own than on adapting their work for differing levels of risk. This is ineffective and inefficient.

2. Supplemental guidance to AS 2 has encouraged the external auditor to properly consider information from prior years in designing their audit testing. While the concept is well described in the guidance, the examples shown for application are overly narrow. For example, question #44 from the Staff Questions and Answers from the PCAOB states that audit knowledge obtained in prior years should not be ignored. However, the only examples of where prior year audit knowledge is used is (1) reducing a sample size for testing and (2) the amount of time spent performing the annually required steps. We observe that external auditors also agree broadly with the concept of adjusting the extent of testing based on prior year audit results, but make few changes to actual work performed, focusing more on the clearly stated requirements for every year to stand on its own.

3. External auditors should include, in their top-down and risk-based approach, an assessment of likely fraud schemes by focusing on fraud that may result in material misstatement. In addition, internal and external auditors should coordinate work to detect fraudulent financial reporting and consideration should be given to integrating SAS 99 work with the §404 work to ensure unpredictability related to material fraud misstatement.

4. We agree that the projection of controls to a future period is problematic; however, the concept of projecting of controls to future periods is germane to investors. We believe that investors are inclined to rely on evidence of the operation of controls in the period right after the annual year-end assessment

because they are more relevant to an assessment as of year-end than activities 180 days before year-end. Stakeholders need to know if internal controls are sufficient to provide comfort not only with respect to the current financials but to future financials, as well.

G. SAS 70 type II reports should be updated and improved by service providers so that clients receive increased reliability and management is considered the target audience of the report instead of the current auditor-to-auditor presentation. These reports should also be discussed with clients of the service providers to ensure they address all relevant clients' needs; be provided at intervals appropriate to clients' assessment needs; and include audits results of remedied items promptly. In addition, client-company management may need to arrange additional testing at the service provider that is not addressed by the SAS70 type II reports.

---

[i] The failure could be individual or together with other controls that are likely to fail at the same time. This is given the term "aggregation" in the literature. While the failure of one control may not be likely to result in a material misstatement, several may fail at the same time, increasing the risk to more than remote. The key is that the controls have to be likely to fail at the same time, for example, because they are performed at the same time by the same people or are using the same computer system.

[ii] The *timely* detection of an error is critical. Otherwise, detection may occur after the financial statements have been filed with the SEC, leading to the potential need for restatement