3701 Algonquin Road, Suite 1010
Rolling Meadows, Illinois 60008, USA
Telephone: 847.253.1545
Facsimile: 847.253.1443
Web Sites: *www.isaca.org* and *www.itgi.org*

27 April 2006

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

and

Office of the Secretary
Public Company Accounting Oversight Board
1666 K Street NW
Washington, DC 20006-2803

Via e-mail to *rule-comments@sec.gov* and *comments@pcaobus.org*

RE: File Number 4-511

Dear SEC and PCAOB Board Members:

We very much appreciate the opportunity to provide comments and recommendations to the Securities and Exchange Commission (SEC) and the Public Company Accounting Oversight Board (PCAOB) on lessons learned from the first two years of applying the Sarbanes-Oxley Act's internal control reporting requirements, including how the efficiency and effectiveness of those assessments and audits could be improved.

These comments and recommendations are offered on behalf of both ISACA and the IT Governance Institute (ITGI), international independent thought leaders on IT governance, controls, security and assurance. A brief description of the organizations is provided at the end of this letter.

ISACA Survey Results

In April 2006, ISACA conducted an online survey of its North American members, who are primarily IS audit and control professionals, and other individuals who participated in recent ISACA Sarbanes-Oxley symposia. The survey addressed issues surrounding their organizations' year-two experiences related to Sarbanes-Oxley compliance. Responses were received from approximately 740 individuals. The summarized findings of the survey form the basis of our comments and recommendations in this letter, and the full survey results are attached.

Primary Comments
Based on our review of the ISACA survey results, the following primary comments were identified:

- Additional guidance for management is needed.
- The risk-based, top-down approach had nominal impact.
- Further IT controls guidance is needed.
- Internal control sustainability is starting to grow as a benefit of Sarbanes-Oxley**.**
- Research on automating key controls is needed.

The following paragraphs summarize key findings from the survey in support of the primary comments listed above.

Additional Guidance for Management is Needed
The survey asked if the respondents perceived a need for additional management-focused guidance on Sarbanes-Oxley 404 compliance. More than 80 percent of the respondents either agreed or strongly agreed that such additional management-focused guidance is needed (question number 1). This area was further supported by the 73 percent who felt that the time is right for separate guidance for management of issuers and for public accountants (question number 3).

> **Recommendation:** ***The SEC should work through COSO and other organizations to ensure additional management-focused guidance on Sarbanes-Oxley 404 compliance is developed and made available.***

The survey respondents identified the following as the top four areas in which additional management-focused guidance is needed:

- IT controls (e.g., access, application, change and security)
- Testing (e.g., requirements, plans, methodologies and sample size)
- Scoping (e.g., risk assessment, relationship to other controls, processes and subprocesses)
- Various definitions (e.g., key controls, application and general controls)

Risk-based, Top-down Approach Had Nominal Impact
More than 60 percent of the respondents indicated that the SEC/PCAOB guidance issued in May 2005, recommending a risk-based, top-down approach, did reduce the scope of management's 404 work in year two (question number 2). However, 33 percent indicated that it did so by less than 5 percent. Nearly 17 percent reported that it actually increased the scope of management's work.

> **Recommendation:** ***The SEC and PCAOB should work through COSO and other organizations to provide additional guidance, illustrations and best practices addressing how to apply the risk-based, top-down, approach.***

This finding is consistent with several other surveys released recently by the CRA International[1] and Financial Executives International (FEI).[2] It appears that the overall resources required have been reduced in year two; however, the exact reasons why are not clear. It is apparent the level of work performed internally at many issuers is decreasing as they focus on Sarbanes-Oxley as part of

[1] *www.crai.com*
[2] *www.fei.org*

a process, and begin to look at their IT risks and controls in the broader context of their IT governance efforts.

Further IT Controls Guidance is Needed

Respondents were asked to identify their best source for addressing IT controls in year two (question number 4); more than 54 percent indicated that they relied on *IT Control Objectives for Sarbanes-Oxley*, published by the IT Governance Institute. Another 46 percent said they utilized an internally developed approach, while 34 percent used the advice of their external audit firm.

> **Recommendation:** ***The SEC and PCAOB should work through COSO to provide additional guidance on IT controls. The starting point for developing this guidance could be the broadly accepted ITGI publication,*** **IT Control Objectives for Sarbanes-Oxley.**

When respondents were asked what IT governance/control framework was used for year two (question number 11), 58 percent indicated they relied on *Control Objectives for Information and related Technology* (COBIT) and 30 percent pointed to *IT Control Objectives for Sarbanes-Oxley.*[3] COSO was used by 36 percent and internally developed approaches by 26 percent. More than 52 percent reported that their IT control framework was easy to use (question number 12).

Internal Control Sustainability is Starting to Grow as a Benefit of Sarbanes-Oxley

More than 57 percent of those responding to the ISACA survey indicated that sustainability was addressed as part of their year-two processes or as part of their year-three planning (question number 19). As a result of Sarbanes-Oxley compliance activities, enterprises are making internal control and sustainability a part of their business processes. Additionally, more than 54 percent reported that their overall sustainability efforts included the need for an IT control framework (question number 20). In the organizations' year-two efforts, more than 50 percent of their sustainability efforts considered business process, process controls and IT control changes (question number 21).

> **Recommendation:** ***The SEC and PCAOB should work through COSO and other organizations to support additional research into best practices and the benefits of sustainability, including a focus on continuous monitoring and auditing.***

Research on Automating Key Controls is Needed

Two-thirds of the respondents indicated that less than 25 percent of their key controls were considered automated in year two (question number 23). The possibility exists that the remaining 75 percent could achieve additional benefits by automating key controls. As more and more key controls are automated, the amount of work should continue to decline for testing and other compliance-related activities and the effectiveness of controls should increase. Looking at the issue slightly differently, 44 percent of respondents indicated that there was an overall increase in the automation of key controls from year one to year two (question number 24).

[3] Both COBIT and *IT Control Objectives for Sarbanes-Oxley* are openly available to the general public from the ISACA and ITGI web sites, *www.isaca.org* and *www.itgi.org.* The draft of the second edition of *IT Control Objectives for Sarbanes-Oxley* will be posted on both sites for public exposure comments from 1 May to 30 June 2006.

Recommendation: ***The SEC and PCAOB should work through COSO and other organizations to support additional research into best practices for automating key controls.***

A Summary of Additional Survey Findings

The following list summarizes key findings from the survey questions not already referenced in the paragraphs above. The list is organized by question number. Questions 22 and 25 were open-ended questions and generated a significant number of essay-type responses. Those results, which are under further analysis, are not included here.

5. Almost half of the respondents reported that no time or less than 5 percent of time was saved for the 404 attestation by having the organization's management work closer with its public accounting firm.
6. More than 50 percent of respondents reported that their public accounting firm took entity-level controls into account in determining their level of testing in year two (question 6.1). For 70 percent of those responding to the question, the reduction in work expended by the accounting firm by utilizing an entity level approach was less than 5 percent (question 6.2).
7. More than 40 percent of the responding organizations used software to assist with 404 compliance. Many respondents wrote in the name of the software program(s) they used, but no particular program(s) dominated the responses. In fact, the top three most often named constituted only 5 percent of the overall replies.
8. More than 40 percent of the respondents indicated that the year-two testing approach differed from the year-one testing approach with regard to scope and number of tests. This may explain why year-two costs have not decreased as much as anticipated.
9. E-mail systems are used by 84 percent of respondents to evidence approvals. Of that 84 percent, almost 60 percent did not include the e-mail system in the scope of Sarbanes-Oxley. Additional guidance is needed on the role of controls in these kinds of situations and the extent, if any, to which such controls need to be documented and tested by management and audited by the external auditor.
10. More than 78 percent of those who replied to the question asking about the organization's IT approach adopted the same level of IT control for smaller subsidiaries as for larger subsidiaries. (Note: This percentage is based on excluding the "not applicable" responses.) There may be an opportunity to use differentiated approaches based on size, top-down approach, risk and other factors. This could lead to potential cost reductions.
13. More than 56 percent stated that their staff obtained in-house training on using their IT control framework.
14. Of the 620 respondents who relied on external expertise to implement the IT control framework, 35 percent used a consultant, 35 percent used a Certified Information Systems Auditor (CISA) or Certified Information Security Manager (CISM), and almost 30 percent used an external auditor.
15. More than 37 percent of respondents changed their IT control framework from year one to year two.
16. More than 73 percent use spreadsheets as an integral part of the financial reporting process.
17. Almost 53 percent use software developed by end users as an integral part of the financial reporting process.
18. Only 15 percent use or adapt the nine-firm (public accounting firms) "Conclude framework" to address general computer controls and potential deficiencies.

26. In year two, more than 58 percent of organizations increased emphasis in testing application controls.
27. Additional comments related to their organizations' experiences in year two were provided by 237 respondents:
    - More than 28 percent are concerned with external audit and inconsistent guidance.
    - More than 15 percent are concerned with cost.
    - More than 10 percent are concerned with testing.
    - More than 5 percent focused on framework issues.

With more than 50,000 members in more than 140 countries, ISACA is a recognized worldwide leader in IT governance, control, security and assurance. Founded in 1969, ISACA sponsors international conferences, publishes the *Information Systems Control Journal*, develops international information systems auditing and control standards, and administers the CISA designation, earned by more than 44,000 professionals since inception, and the CISM designation, a groundbreaking credential earned by 5,500 professionals in its first three years.

The IT Governance Institute (ITGI) was established by ISACA in 1998 to advance international thinking and standards in directing and controlling an enterprise's information technology. ITGI developed *Control Objectives for Information and related Technology* (COBIT), now in its fourth edition, and offers original research and case studies to assist enterprise leaders and boards of directors in their IT governance responsibilities.

Thank you for this opportunity to relay our comments on the lessons learned from the first two years of applying the Act's internal control reporting requirements. Because ISACA and ITGI represent many of the individuals engaged in Sarbanes-Oxley compliance efforts and much of the guidance informing those efforts, we believe we are uniquely positioned to bring value to any future projects to address our recommendations. Please feel free to call on us if we can be of assistance in any way in task forces, committees or work groups. Representatives of ISACA and ITGI will be present at the SEC and PCAOB Roundtable meeting on 10 May in Washington and we look forward to the discussion of these issues.

Respectfully submitted,

Everett C. Johnson, CPA
2005-2006 International President
ISACA (*www.isaca.org*)
IT Governance Institute (*www.itgi.org*)

cc: Mr. Larry Rittenberg, Chairman, COSO Board, via e-mail to *lrittenberg@bus.wisc.edu*

Attach: ISACA survey results

3701 Algonquin Road, Suite 1010
Rolling Meadows, Illinois 60008, USA
Telephone: 847.253.1545
Facsimile: 847.253.1443
Web Sites: *www.isaca.org* and *www.itgi.org*

Preliminary ISACA Survey Results

With more than 50,000 members in more than 140 countries, ISACA is a recognized worldwide leader in IT governance, control, security and assurance. Founded in 1969, ISACA sponsors international conferences, publishes the *Information Systems Control Journal*, develops international information systems auditing and control standards, and administers the CISA designation, earned by more than 44,000 professionals since inception, and the CISM designation, a groundbreaking credential earned by 5,500 professionals in its first three years.

The IT Governance Institute (ITGI) was established by ISACA in 1998 to advance international thinking and standards in directing and controlling an enterprise's information technology. ITGI developed *Control Objectives for Information and related Technology* (COBIT), now in its fourth edition, and offers original research and case studies to assist enterprise leaders and boards of directors in their IT governance responsibilities.

The following results were generated from an online survey posted from 12 to 15 April 2006. The survey addressed issues surrounding organizations' year-two experiences related to Sarbanes-Oxley compliance. ISACA members in North America, who are primarily IS audit and control professionals, and participants in recent ISACA symposia on Sarbanes-Oxley were invited to complete the survey. Responses were received from approximately 740 individuals.

The charts below represent the statistical results of the survey. Questions 22 and 25, which were open-ended questions, generated a significant number of essay-type responses. Those responses are still being analyzed and are therefore not included in this document.

1. Do you think additional guidance for 404 compliance, directed at management of companies, would be helpful?			
	Counts	Percents	Percents 0 100
Strongly Agree	335	45.2%	
Agree	268	36.2%	
Disagree	82	11.1%	
Strongly Disagree	15	2.0%	
Not Applicable	41	5.5%	
Totals	741	100.0%	
Mean	3.32		

Top four topics suggested for additional guidance were:

- 292 on controls
- 105 on testing
- 84 on scoping
- 74 on definitions

2. Did the SEC/PCAOB guidance issued in May 2005, recommending a risk based, top down, approach reduce the scope of managements' 404 work?			
	Counts	Percents	Percents 0 100
Less than 5%	247	33.3%	
Increased work	124	16.7%	
6 to 10%	94	12.7%	
More than 15%	72	9.7%	
11 to 15%	40	5.4%	
Not Applicable	164	22.1%	
Totals	741	100.0%	
Mean	--		

3. Do you believe there is a need for separate guidance for issuers and public accounting firms?			
	Counts	Percents	Percents 0 100
Strongly Agree	265	35.8%	
Agree	277	37.4%	
Disagree	103	13.9%	
Strongly Disagree	44	5.9%	
Not Applicable	52	7.0%	
Totals	741	100.0%	
Mean	3.11		

4. In year two, what was your best source for addressing IT controls? (If more than one used, please check the top two only)			
	Counts	Percents	Percents 0 100
IT Control Objectives for Sarbanes-Oxley	403	54.4%	
Internal developed approach	343	46.3%	
External audit firm	255	34.4%	
Other external guidance	93	12.6%	
No adequate guidance available	62	8.4%	
Not Applicable	12	1.6%	
Totals	741	n/a	
Mean	--		

5. How much time was saved for the 404 attestation by having your organization's management working closer with your public accounting firm?			
	Counts	Percents	Percents 0 100
None	200	27.0%	
Less than 5%	143	19.3%	
More than 15%	111	15.0%	
6% to 10%	87	11.7%	
11% to 15%	54	7.3%	
Not Applicable	146	19.7%	
Totals	741	100.0%	
Mean	--		

6.1 Did your public accounting firm take into account entity level controls in determining their level of testing in year two?			
	Counts	Percents	Percents 0 100
Strongly Agree	84	11.3%	
Agree	321	43.3%	
Disagree	134	18.1%	
Strongly Disagree	51	6.9%	
Not Applicable	151	20.4%	
Totals	741	100.0%	
Mean	2.74		

6.2 What was the impact (reduction in work) to amount of work expended by your accounting firm by utilizing an entity level approach?			
	Counts	Percents	Percents 0 100
None	186	25.1%	
Less than 5%	185	25.0%	
6% to 10%	87	11.7%	
More than 15%	39	5.3%	
11% to 15%	28	3.8%	
Not Applicable	216	29.1%	
Totals	741	100.0%	
Mean	--		

7. Did your organization use software to assist with 404 compliance?			
	Counts	Percents	Percents 0 100
No	394	53.2%	
Yes	299	40.4%	
Not Applicable	48	6.5%	
Totals	741	100.0%	
Mean	--		

8. The testing approach in year two differed from the testing approach used in year one by: (please check the top two only, if more than one applies)			
	Counts	Percents	Percents 0 100
Scope	374	50.5%	
Number of tests	320	43.2%	
Method of testing	207	27.9%	
None	110	14.8%	
# of controls tested	1	0.1%	
A reduced number of 'canned' checklists being used	1	0.1%	
Additional Testing	1	0.1%	
All of the above - scope, method of testing, number of tests	1	0.1%	
Being able to rely on managements work if proper standards were applied.	1	0.1%	
Client tried to manipulate control wording instead of addressing the issues. Control framework went through more than 12 major revisions. (ie a moving target)	1	0.1%	
General Efficiency due to client controls in place and remediation testing greatly reduced	1	0.1%	
Improved quality and detail	1	0.1%	
Internal Audit performed testing in Year 2 on behalf of Management	1	0.1%	
Knew better what the externals were looking for	1	0.1%	
Less baseline testing required, otherwise similar	1	0.1%	

9. If you used e-mail to evidence approvals did you include the e-mail system in the scope of Sarbanes-Oxley?			
	Counts	Percents	Percents 0 100
No	425	57.4%	
Yes	198	26.7%	
Not Applicable	118	15.9%	
Totals	741	100.0%	
Mean	--		

10. Regarding your organization's IT approach, did you adopt the same standard of control for smaller subsidiaries as for larger subsidiaries or did your organization utilize the draft COSO for Small			
	Counts	Percents	Percents 0 100
Same	435	58.7%	
COSO for Small Business	54	7.3%	
Not Applicable	5	0.7%	
CobIT	3	0.4%	
no subsidiaries	3	0.4%	
Materiality	2	0.3%	
A mix of the COSO for small buisness as well as a risk based approach	1	0.1%	

[Continuing table]

10. Regarding your organization's IT approach, did you adopt the same standard of control for smaller subsidiaries as for larger subsidiaries or did your organization utilize the draft COSO for Small			
	Counts	Percents	Percents 0 100
As an internal consultant we did not have a choice here as the external auditors come in with their own control objctives that do not alter depedent on the size of business or industry.	1	0.1%	
Both started with COSO but applied with different methods	1	0.1%	
Client attempted to eliminate small subsidiaries and aquistions.	1	0.1%	
Cobit small business	1	0.1%	
COSO, CoBIT, ITIL, ITGI	1	0.1%	
Different approach	1	0.1%	
Different based on risk and size of business	1	0.1%	
Divided all subsidiaries into Tiers, based upon size.	1	0.1%	
Other	41	5.5%	
Not Applicable	189	25.5%	
Totals	741	100.0%	
Mean	--		

11. What IT governance/control frameworks did your company use for year two? (If more than one used, please check the top two only.)			
	Counts	Percents	Percents 0 100
COBIT	428	57.8%	
COSO	270	36.4%	
IT Control Objectives for Sarbanes-Oxley	226	30.5%	
Internally developed	195	26.3%	
ISO17799	50	6.7%	
Experience	50	6.7%	
ITIL	27	3.6%	

[Continuing table]

11. What IT governance/control frameworks did your company use for year two? (If more than one used, please check the top two only.)			
	Counts	Percents	Percents 0 100
ITCG	8	1.1%	
Not Applicable	14	1.9%	
Totals	741	n/a	
Mean	--		

12. How easy or difficult was the IT control framework to use?			
	Counts	Percents	Percents 0 100
Easy	345	46.6%	
Difficult	279	37.7%	
Very easy	39	5.3%	
Very difficult	26	3.5%	
Not Applicable	52	7.0%	
Totals	741	100.0%	
Mean	--		

13. Where did your staff obtain training on using the IT control framework?

	Counts	Percents	Percents 0 100
In house	420	56.7%	
Outsourced	120	16.2%	
Certification	106	14.3%	
Not Applicable	95	12.8%	
Totals	741	100.0%	
Mean	--		

14. The type of external expertise relied on to implement the IT control framework was:

	Counts	Percents	Percents 0 100
Consultant	222	30.0%	
CISA	198	26.7%	
External auditor	183	24.7%	
CISM	17	2.3%	
Not Applicable	121	16.3%	
Totals	741	100.0%	
Mean	--		

15. Did you change the IT control framework from year one to year two?

	Counts	Percents	Percents 0 100
No	384	51.8%	
Yes	277	37.4%	
Not Applicable	80	10.8%	
Totals	741	100.0%	
Mean	--		

16. Are spreadsheets used as an integral part of the financial reporting process?

	Counts	Percents	Percents 0 100
Yes	547	73.8%	
No	130	17.5%	
Not Applicable	64	8.6%	
Totals	741	100.0%	

[Continuing table]

16. Are spreadsheets used as an integral part of the financial reporting process?			
	Counts	Percents	Percents 0 100
Mean	--		

17. Is end user developed software used as an integral part of the financial reporting process?			
	Counts	Percents	Percents 0 100
Yes	389	52.5%	
No	280	37.8%	
Not Applicable	72	9.7%	
Totals	741	100.0%	
Mean	--		

18. Has the 9 firm (public accounting firms) "Conclude framework" been used or adapted to address general computer controls and potential deficiencies?			
	Counts	Percents	Percents 0 100
No	256	34.5%	
Yes	115	15.5%	
Not Applicable	370	49.9%	
Totals	741	100.0%	
Mean	--		

19. Was sustainability addressed as part of the year two processes or part of year three planning?			
	Counts	Percents	Percents 0 100
Yes	425	57.4%	
No	162	21.9%	
Not Applicable	154	20.8%	
Totals	741	100.0%	
Mean	--		

20. Did sustainability include the need for an IT controls framework?			
	Counts	Percents	Percents 0 100
Yes	403	54.4%	
No	153	20.6%	
Not Applicable	185	25.0%	
Totals	741	100.0%	
Mean	--		

21. In your organizations year two efforts, did your sustainability efforts consider?			
	Counts	Percents	Percents 0 100
IT control changes?	399	53.8%	
process controls	391	52.8%	
business process,	373	50.3%	
certification process	1	0.1%	
Change in SBU Functional Role within the corporation	1	0.1%	
Changes to people, processes, IT, and materiality	1	0.1%	
Client just wanted to complete the paperwork with no thought of the future	1	0.1%	
Company acquisitions	1	0.1%	
document management	1	0.1%	
Focused on doing the same tests, but reducing sample size	1	0.1%	
I have been trying since 2003 to get the organization to comply with SOX, they have yet to do so,.	1	0.1%	
key control scoping changes	1	0.1%	
Most leaders are a tad dense and think SOX is just a project. PM rotated on/off and no one thought about it again until 3Q05.	1	0.1%	

[Continuing table]

21. In your organizations year two efforts, did your sustainability efforts consider?	Counts	Percents	Percents 0 100
no	1	0.1%	
No sustainability was considered.	1	0.1%	
Other	12	1.6%	
Not Applicable	204	27.5%	
Totals	741	n/a	
Mean	--		

22. If your organization relied on manual controls for information generated by computer-based reports, how was the evaluation and reporting of manual control procedures integrated with IT controls? Responses still being analyzed.

23. In year two, what percentage of key controls that your organization identified were considered 'automated" key controls?	Counts	Percents	Percents 0 100
11% to 25%	235	36.8%	
Less than 10%	196	30.7%	
26% to 50%	137	21.4%	
More than 50%	71	11.1%	
Totals	639	100.0%	
Mean	--		

24. Was there an increase in the automation of key controls in year two versus year one?	Counts	Percents	Percents 0 100
Strongly Agree	36	4.9%	
Agree	288	39.0%	
Disagree	252	34.1%	
Strongly Disagree	54	7.3%	
Not Applicable	108	14.6%	
Totals	738	100.0%	
Mean	2.49		

25. Describe any other significant trends in the results of control testing and subsequent evaluations. Responses still being analyzed.

26. In year two, did your organization increase its emphasis in testing application controls?			
	Counts	Percents	Percents 0 100
Strongly Agree	73	9.9%	
Agree	360	48.6%	
Disagree	195	26.3%	
Strongly Disagree	37	5.0%	
Not Applicable	76	10.3%	
Totals	741	100.0%	
Mean	2.71		

27. Additional comments related to their organizations' year-two experiences were provided by 237 respondents:
    - More than 28 percent are concerned with external audit and inconsistent guidance.
    - More than 15 percent are concerned with cost.
    - More than 10 percent are concerned with testing.
    - More than 5 percent focused on framework.