Sarbanes Oxley Section 404 Transformational Guidance to Help Company Management "Get it Right"

Institute of Management Accountants

SOX Advisory Overview

CMA CERTIFIED MANAGEMENT ACCOUNTANT
Professionals Driving Business Performance™

IMA INSTITUTE OF MANAGEMENT ACCOUNTANTS
Advancing the Profession™

SOX 404 Root Cause

Chairman Cox, May 2006

- "Auditing Standard No. 2 (AS 2) gives guidance to independent auditors tasked with determining whether a company's internal controls are effective. *No similar guidance, however, exists for companies and for their management*. And in the absence of direction from us, companies have been basing the assessment of their controls on AS 2 …."

More on the SOX 404 Root Cause

SEC Concept Release, July 2006

- "While the COSO framework provides an integrated framework that identifies components and objectives of internal control, it does not set forth detailed guidance as to the steps that management must follow in assessing the effectiveness of a company's ICoFR. We, therefore, *distinguish between the COSO framework as an internal control framework and other forms of guidance that illustrate how to conduct an assessment of the effectiveness* of ICoFR."

SOX 404: The Good, the Not so Good, The Path Forward

The Act (Law) itself was a good thing. Why?

- Shareholder confidence restored (for the most part).
- Renewed corporate emphasis on internal controls, business process management and ethics.
- Even non-publicly traded companies have this renewed emphasis on behalf of their stakeholders.

SOX: The Good, the Not so Good, The Path Forward

The Implementation Guidance has been a disaster. Why?

- AS2 is audit and control centric – Test and document everything that "moves" regardless of risk to achieve the objective of materially fault-free financial statements.
- No practical management assessment guidance exists, resulting in costly patchwork processes with expensive consultants involved and full time corporate staffs.
- Most of the frameworks, tools and training were written by auditors for auditors vs. management responsible for financial reporting, internal controls and driving business performance.
- Disproportionate impact on the lifeblood of the U.S. economy – smaller businesses – resulting in "bad" solutions vs. developing cost effective and scalable management assessment guidance.

SOX: The Good, the Not so Good, The Path Forward

- Develop Transformational Management Guidance which
  - Draws on global quality and risk disciplines.
  - Is practical, risk-based (to determine "key" controls) and scalable.
  - Is "controls framework neutral" to drive global harmonization.
  - Puts accountability in the hands of management.
  - Is supplemented by tools, training and certification for management.
- Eliminate the Pass/Fail External Audit Opinion on the Effectiveness of Management's ICoFR.
- Eliminate the Language that Requires the Assessment be done in accordance with a single "suitable" framework.
- Modify Auditing Standard No. 2 AFTER new management guidance is written, not before.

SOX: The Path Forward

Transformational Management Guidance must:

- Be Risk-based and draw on global advances in the field of ERM (Enterprise Risk Management).
  - Example: Aussie/NZ Standard 4360,
  - A disciplined risk-based approach *implemented by management* results in testing/documentation of controls and performance indicators only if there is an unacceptable risk of not achieving the business objective: materially fault free financial statements and disclosures.
  - Auditors must get trained in "risk based" approaches – this could result in *l*ess auditor liability, lower overall costs, and more accountability in the hands of company management.

SOX: The Path Forward

Transformational Management Guidance must:

- Draw on principles and advances in the field of global Quality Management
  - Example: Malcolm Baldrige National Quality Award.
  - Measurement of continuous improvement vs. subjective and costly binary yes/no "effectiveness" conclusions required by auditors and management.
  - Measurement of historical error rates in financial statements and processes are critical in addressing the costly question "how much control is enough"?
  - Building quality in, not on (after the fact) is the mantra …, and yet, major global associations involved in Risk and Quality disciplines are not at the "SEC table".....but the audit firms are all over the place.

SOX: The Path Forward

The major recommended guidance change is to eliminate the requirement that auditors and management, independent of each other, develop a binary "yes/no" effectiveness conclusion on the company's system of internal controls over financial reporting. This regime has resulted in subjective and unproductive debate, costly and unnecessary over-auditing and testing, and, has actually increased litigation risk to auditors and management … *continued*

SOX: The Path Forward

(continued) … **The current guidance on this matter would be replaced** by management and auditor's seeking consensus agreement on ***management's*** assessment of the current level of risk remaining after controls are in place, as well as auditor's opining on the risk assessment process management has in place. This change would result in significantly lower costs and audit liability, and put primary accountability where it belongs – in the hands of company management.

APPENDIX

A Global Perspective on ICoFR

Key theme in the IMA recommendations:

Disclosed residual risk status

vs.

Subjective "effective"/"adequate" opinion on ICoFR from external auditors and CEOs and CFOs

CMA CERTIFIED MANAGEMENT ACCOUNTANT
Professionals Driving Business Performance™

IMA INSTITUTE OF MANAGEMENT ACCOUNTANTS
Advancing the Profession™

A Global Perspective on ICoFR

Current SEC/PCAOB rules —

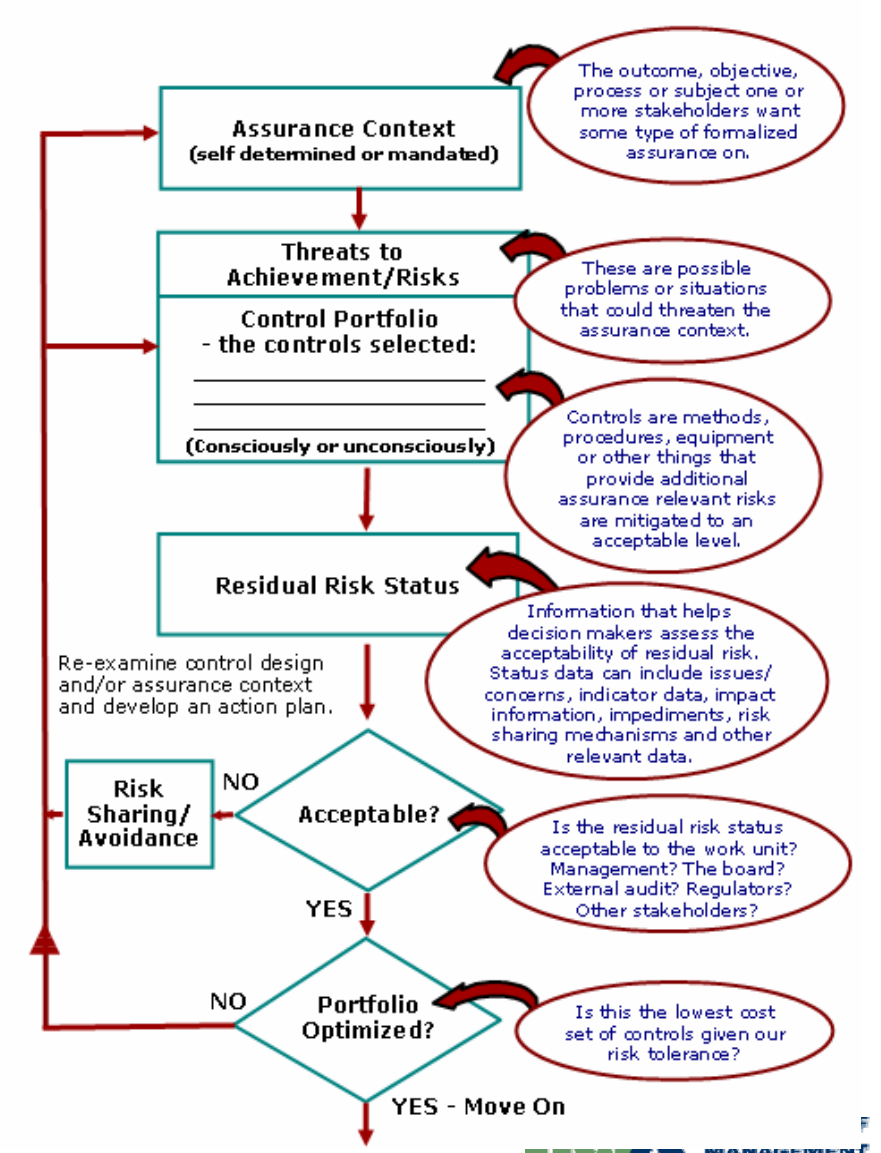
Pretend that external auditors have not historically played a key role in ICoFR in public companies.

This is a major issue for SMBs that have relied on external audit for the final inspection and “rework”.

Core Components of a Risk-Based Approach

This approach can be used:

- At the entity level
- At the subsidiary level
- For accounts
- For processes that support accounts
- For note disclosures



CMA CERTIFIED MANAGEMENT ACCOUNTANT
Professionals Driving Business Performance™

IMA MANAGEMENT ACCOUNTANTS
Advancing the Profession™

A Global Perspective on ICoFR

Top-Down/Risk-Based ICoFR

Create a universe of "Assurance Contexts".

Start with the entity level assurance context — "reliable auditor certified financial disclosures" and cascade down to significant sub-components.

Do not neglect financial statement note disclosure.

A Global Perspective on ICoFR

Top-Down/Risk-Based ICoFR

Assurance Universe Risk Scoring Criteria

1. Detected error history – external auditor
2. Detected error history – management detected after release of statements
3. Absolute dollar/unit of local currency value/impact of location/account
4. Detected error history – regulators/tax authorities/customers/others
5. Detected error history – internal audit
6. Detected/known errors in other companies in the same business sector

A Global Perspective on ICoFR

Top-Down/Risk-Based ICoFR

Assurance Universe Risk Scoring Criteria

7. Amount of management judgment/subjectivity
8. Importance of account/location to security analysts
9. Importance of account/note disclosure to debt covenants
10. Susceptibility of account to fraud from insiders
11. Susceptibility of account to fraud from outsiders
12. Account/note linkage to the company's reward/compensation system

A Global Perspective on ICoFR

Top-Down/Risk-Based ICoFR

Techniques to Identify Risks

1. Research and observation
2. Company specific history
3. Experience of staff
4. Industry specific scenario analysis
5. Risk source analysis
6. Industry "checklists"

A Global Perspective on ICoFR

Top-Down/Risk-Based ICoFR

Techniques to Analyze Risks

Major risks should receive the most attention.

Real risks to financial statement reliability did not receive the attention they deserved in many companies.

e.g. CEO/CFO compensation massively rewards profit manipulation.

A Global Perspective on ICoFR

Top-Down/Risk-Based ICoFR

Treat/Mitigate Risks

BIG PICTURE TACTICS

AVOID — viable strategy for F/S disclosure reliability

MITIGATE — excessive emphasis in AS2 on "direct" controls

SHARE — not understood by accountants

ACCEPT — AS2 does not allow

A Global Perspective on ICoFR

Top-Down/Risk-Based ICoFR

Treat/Mitigate Risks

Using COSO 1992

Using COSO SPC

Using CoCo/Cadbury

Using CARD®*model*

Using COBIT/ISO 17799 / 27001

Emphasis should be on design analysis and "the human element"

CMA CERTIFIED MANAGEMENT ACCOUNTANT
Professionals Driving Business Performance™

IMA INSTITUTE OF MANAGEMENT ACCOUNTANTS
Advancing the Profession™

A Global Perspective on ICoFR

Top-Down/Risk-Based ICoFR

Control confirmation — Over emphasized in AS2

Massively expensive
$ $ $ $ $ $

Start by asking control sponsors and obtaining electronic signature

Sample test control sponsor representations

Severe consequences for conscious deceit

CMA CERTIFIED MANAGEMENT ACCOUNTANT
Professionals Driving Business Performance™

IMA INSTITUTE OF MANAGEMENT ACCOUNTANTS
Advancing the Profession™

A Global Perspective on ICoFR

Top-Down/Risk-Based ICoFR

Identify and analyze RESIDUAL RISK STATUS — Under emphasized

- Concerns (unmitigated risks)
- Indicator data
- Impact data
- Impediment data
- Transfer/Risk sharing

A Global Perspective on ICoFR

Global Regulatory Considerations

1. Form and content of management representation
2. Form of auditor assurance on ICoFR
3. Grading control deficiencies
4. Mandatory ICoFR
5. Mandatory use of COSO 92

A Global Perspective on ICoFR

The Future — Impact on Other Countries

Key issue —

Will U.S. listed companies have "GRADE A" audit opinions and other countries have Grade B, C, D audit opinions?

or

Is the SEC just forcing registrants to waste shareholder money?