PAISLEY CONSULTING

Business accountability solutions.

"Top-Down/Risk-Based" SOX Assessment:

How to Negotiate a Lower Cost of Compliance

April 20, 2006

parson consulting

PAISLEY CONSULTING

Business accountability solutions.

Agenda

- Introductions
- The Root Cause Problem
- Top-Down/Risk-Based Demand Drivers
- Top-Down/Risk-Based Assessment Methods
- SOX Cost Reduction Strategies

parson consulting

PAISLEY CONSULTING

Business accountability solutions.

Introductions

- **Paisley Consulting:** an industry leading independent software vendor that provides solutions for audit automation, Sarbanes-Oxley compliance, operational risk management and general compliance.

parson consulting

PAISLEY CONSULTING

Business accountability solutions.

Introductions

- **Parson Consulting:** Parson Consulting focuses on helping senior finance executives improve the efficiency and effectiveness of finance and other support functions. Parson Consulting specializes in Strategic Finance, Accounting & Finance Operations, Governance & Risk Management and Sarbanes-Oxley, and Corporate Transactions (M&A).

parson consulting

PAISLEY CONSULTING

Business accountability solutions.

The Root Cause Problem

- The SEC says they want "TOP-DOWN/ RISK-BASED" SOX assessments.
- Many people, including external auditors, believe PCAOB AS#2 calls for BOTTOM-UP/CONTROL-CENTRIC assessments.

parson consulting

PAISLEY CONSULTING

Business accountability solutions.

The Root Cause Problem

- There is no SEC sanctioned SOX 302/404 guidance for public companies that describes how to actually do TOP-DOWN/RISK-BASED assessments.
- The global cost of doing BOTTOM-UP/ CONTROL-CENTRIC assessments is enormous.

parson consulting

PAISLEY CONSULTING

Business accountability solutions.

The Root Cause Problem

- SEC & PCAOB rules related to SOX 302/404 are under attack on multiple fronts.

parson consulting

PAISLEY CONSULTING

Business accountability solutions.

Top-Down/Risk-Based ("TD/RB") Demand Drivers

Current Situation Simplified Using a Personal Health Analogy:

PCAOB AS #2, as it stands today, requires the equivalent of a mandatory annual physical check-up with a massive number of diagnostic steps and tests — regardless of the patient's health history, age or symptoms.

parson consulting

PAISLEY CONSULTING

Business accountability solutions.

TD/RB Demand Drivers

Current Situation Simplified Using a Personal Health Analogy:

This assessment approach has resulted in massive costs and time outlays, business disruption, eroding U.S. competitiveness, and widespread rejection of the value of SOX 404 by the global business community.

parson consulting

PAISLEY CONSULTING

Business accountability solutions.

TD/RB Demand Drivers

"one reason why too many controls and processes were identified, documented and tested was that in many cases neither a top-down nor a risk-based approach was effectively used"

(SEC May 16, 2005 Staff Statement on Management's Report on Internal Control Over Financial Reporting)

parson consulting

PAISLEY CONSULTING

Business accountability solutions.

TD/RB Demand Drivers

"the desired approach should devote resources to the areas of greatest risk and avoid giving all significant accounts and related controls equal attention without regard to risk"

(SEC May 16, 2005 Staff Statement on Management's Report on Internal Control Over Financial Reporting)

parson consulting

PAISLEY CONSULTING

Business accountability solutions.

TD/RB Demand Drivers

"Employing such a top-down approach requires that management apply in a reasonable manner its cumulative knowledge, experience and judgement to identify the areas that present significant risk."

(SEC May 16, 2005 Staff Statement on Management's Report on Internal Control Over Financial Reporting)

parson consulting

©2006 Paisley Consulting. All Rights Reserved

PAISLEY CONSULTING

Business accountability solutions.

TD/RB Demand Drivers

- "the level of testing performed for a low risk account will likely be different than it will be for a high risk account" (Note: it isn't clear why "will likely" was used by the SEC versus "should"
- "management and auditors should keep the "reasonable assurance" standard in mind"

(SEC May 16, 2005 Staff Statement on Management's Report on Internal Control Over Financial Reporting)

parson consulting

PAISLEY CONSULTING

Business accountability solutions.

TD/RB Demand Drivers

"even though auditors maintain they are already taking a risk-based approach to the AS#2 audit, we heard significant testimony from companies suggesting that implementation of AS#2 has resulted in very rigid, prescriptive audits as a result of onerous AS#2 requirements."

(Final Report of the Advisory Committee on Smaller Public Companies to the U.S. SEC)

parson consulting

©2006 Paisley Consulting. All Rights Reserved

PAISLEY CONSULTING

Business accountability solutions.

TD/RB Demand Drivers

"Section 404 had often inappropriately shifted the focus from a top-down, risk-based management perspective to a bottom-up, "check the box" auditor perspective… Nevertheless, I continue to hear more about potential misfocus of the Section 404 process and associated costs."

(Speech SEC Commissioner Cynthia A. Glassman, March 9, 2006 at the 10th Annual Corporate Counsel Institute Conference)

parson consulting

PAISLEY CONSULTING

Business accountability solutions.

TD/RB Assessment Methods

General Principle: "the desired approach should devote resources to the areas of greatest risk" (SEC May 16, 2005)

Problems:

- For SOX 302/404 what does this really mean?
- Does the concept of top-down/risk-based assessment conflict with the existing requirements in PCAOB Auditing Standard No. 2?

parson consulting

PAISLEY CONSULTING

Business accountability solutions.

TD/RB Assessment Methods

General Principle: "the desired approach should devote resources to the areas of greatest risk" (SEC May 16, 2005)

Problems:

- No authoritative guidance for management currently exists describing how to do practical, cost-effective top-down/risk-based disclosure assessments.
- None of the COSO guidance documents — COSO 1992, COSO ERM, or COSO for Smaller Public Companies 2006, provide practical guidance.

parson consulting

PAISLEY CONSULTING

Business accountability solutions.

TD/RB Assessment Methods

Method #1

Since the majority of problems that led to SOX involved senior executives and fraud it makes sense to do a:

Macro level anti-fraud assessment

A survey done by the IMA in January 2006 indicates many companies are skipping this critical/important step and at least some external auditors appear to be accepting the omission.

parson consulting

PAISLEY CONSULTING

Business accountability solutions.

TD/RB Assessment Methods

Method #1	Macro level anti-fraud assessment
Best assessment method:	"Risk Centric"
How to do it:	State plausible, statistically predictable fraud related risks to reliable financial disclosures and describe mitigating controls in place

parson consulting

PAISLEY CONSULTING

Business accountability solutions.

TD/RB Assessment Methods

Method #1 Example	Risk Centric Anti-Fraud
Sample Risk:	CEO, CFO and/or Controller improperly order invalid/improper accounting adjustments
Mitigating Controls:	➢ Audit Committee oversight ➢ Confidential concerns hotline ➢ External auditor COSO evaluation ➢ Code of conduct ➢ Jail sentences, fines, and personal liability ➢ Etc.

parson consulting

PAISLEY CONSULTING

Business accountability solutions.

TD / RB Assessment Methods

Method #1 Example (cont'd)	Risk Centric Anti-Fraud
Sample Risk:	VP Sales creates or condones contract side-deals creating off-book liabilities
Mitigating Controls:	➢ Standard contract clause denying validity of any pre-existing deals and other future side-deals ➢ Corporate code of conduct ➢ Confidential concerns hotline ➢ Independent contract terms confirmation analyst contacts client ➢ Etc.

parson consulting

PAISLEY CONSULTING

Business accountability solutions.

TD / RB Assessment Methods

Method #1	Macro level anti-fraud assessment
Next best assessment method:	Control/Compliance Centric Anti-Fraud assessment
How to do it:	Obtain best available checklist(s) of macro anti-fraud controls and evaluate conformance

parson consulting

PAISLEY CONSULTING

Business accountability solutions.

TD/RB Assessment Methods

Method #1 Example	Control/Compliance Centric Anti-Fraud
Control Criteria:	The organization has documented and communicated standards on truthful and reliable financial reporting
Assessment:	1 2 3 4 5 Limited Evidence … Extensive Evidence

parson consulting

PAISLEY CONSULTING

Business accountability solutions.

TD/RB Assessment Methods

Method #2

Since serious financial disclosure problems that don't involve senior management fraud can often be traced to unintentional errors made during the financial statement preparation phase it makes sense to do a:

Financial Statement Preparation Control Assessment

parson consulting

PAISLEY CONSULTING

Business accountability solutions.

TD/RB Assessment Methods

Method #2	Financial Statement Preparation Control Assessment
Best assessment method:	Process Centric
How to do it:	➢ Identify process objectives ➢ Identify risks ➢ Identify controls ➢ Identify residual risk indicators and concerns ➢ Track process performance and error frequency

parson consulting

PAISLEY CONSULTING

Business accountability solutions.

TD/RB Assessment Methods

Method #2 Example	F/S Preparation Control Assessment
Process Objectives:	➢ Reliable F/S that fairly present ➢ F/S conform to relevant GAAP standards
Risk:	Use wrong/inappropriate accounting treatment for business activity/transaction
Mitigating Controls:	➢ Subscribe to GAAP update service ➢ Qualified professional staff ➢ Staff take annual SEC update training ➢ Disclosure Committee reviews decisions with high judgement/subjectively ➢ CFO review and sign-off ➢ Expert advice/opinions sought on some issues

parson consulting

PAISLEY CONSULTING

Business accountability solutions.

TD/RB Assessment Methods

Method #3

Since many major problems can be traced to situations where senior management and the Board didn't fully understand some aspect of the business and didn't intervene when red flags appeared it makes sense to:

Identify business units/topics/accounts with high complexity and/or judgment

parson consulting

PAISLEY CONSULTING

Business accountability solutions.

TD/RB Assessment Methods

Method #3	Complexity/Judgement Scoring
Best assessment method:	Group evaluation and scoring
How to do it:	➢ Assemble a group with knowledgeable, experienced staff and rate company locations, accounts and notes on complexity/judgement ➢ High scores warrant more detailed formal risk/control assessment documentation and testing ➢ Provide training for senior executives and audit committee on high risk areas

parson consulting

PAISLEY CONSULTING

Business accountability solutions.

TD / RB Assessment Methods

Method #4

Since many major problems can be predicted by analyzing previous material errors detected by external auditors and/or company management it makes sense to do:

Accounting error analysis

Accounting errors are "Key Performance Indicators"

parson consulting

PAISLEY CONSULTING

Business accountability solutions.

TD / RB Assessment Methods

Method #4	Accounting Error Analysis
Best assessment method:	Loss/Incident/Error Database
How to do it:	➢ Establish a materiality threshold ➢ Record, track and analyze all accounting errors/misstatements detected by external auditors and/or by management ➢ Direct more resources to identify root cause(s) in problem areas

parson consulting

PAISLEY CONSULTING

Business accountability solutions.

TD / RB Assessment Methods

Method #5

Since many problems can be traced back to macro level control deficiencies and, most importantly, CEO's and CFO's must personally certify SOX control assessments are done "in accordance with _____" (fill in SEC acceptable control framework) it makes sense to complete a:

Macro control framework assessment

parson consulting

PAISLEY CONSULTING

Business accountability solutions.

TD / RB Assessment Methods

Method #5	Macro Control Assessment
Best assessment method:	Organization-wide survey, workshops, or internal auditor analysis
How to do it:	➢ Select control framework to be used (e.g. COSO 1992, CoCo 1995, COSO ERM, COSO Small Business, etc.) ➢ With respect only to the external financial statement disclosure process use an annual survey or workshop(s) to identify weak areas relative to selected control criteria and evaluate possible impact on reliable financial statements

parson consulting

PAISLEY CONSULTING

Business accountability solutions.

TD/RB Assessment Methods

Method #6

Since many major accounting problems have already happened somewhere else it makes sense to use:

Scenario modelling

parson consulting

PAISLEY CONSULTING

Business accountability solutions.

TD/RB Assessment Methods

Method #6	Scenario Modelling
Best assessment method:	Situation/event logging with link to any internal analysis or vulnerability assessment that has been done
How to do it:	➢ Have someone in the organization subscribe to a service that tracks publicized industry specific frauds, restatements, SEC prosecutions and material weakness disclosures (e.g. Audit Analytics, www.sarbanes-oxley.com) ➢ Log situations that may be relevant to your business and ask the question "Could it happen to us?" and "Would our controls prevent/detect it?" Document link to assessment work done Note: This is also a key element of Method #1

parson consulting

PAISLEY CONSULTING

Business accountability solutions.

TD/RB Assessment Methods

Method #7

Since the people that manage and oversee accounting systems often know, or should know, where the serious risks and problems are, use disclosure account/note disclosure:

High Level Residual Risk Assessments/Ratings

parson consulting

PAISLEY CONSULTING

Business accountability solutions.

TD/RB Assessment Methods

Method #7	Residual Risk Ratings
Best assessment method:	Risk & Control Self-assessment
How to do it:	➢ Assign responsibility for significant accounts, notes and processes ➢ Require disclosure account/note owners/sponsors in each significant business unit complete a high level, risk-based assessment, certify controls, report control deficiencies, and assign a Residual Risk Rating score ➢ Sample test sponsor/owner representations ➢ In cases where this high level assessment approach indicates problems/concerns, complete more detailed risk and control evaluation and testing as appropriate

parson consulting

©2006 Paisley Consulting. All Rights Reserved

PAISLEY CONSULTING

Business accountability solutions.

If PCAOB AS#2 remains unchanged, and no SEC accepted "management centric", top-down/risk-based control assessment framework emerges, methods 1-7 may have to be supplemented with more detailed and expensive bottom-up/control and process centric documentation and testing to meet current PCAOB AS#2 requirements.

parson consulting

PAISLEY CONSULTING

Business accountability solutions.

SOX Cost Reduction Strategies

Issue	Action
• Know the rules, especially the SEC interpretations of the rules and negotiate a "reasonable" approach with your external auditor.	• In this transition period, you may need to seek professional advice.

parson consulting

PAISLEY CONSULTING

Business accountability solutions.

SOX Cost Reduction Strategies

Issue	Action
• Make sure your SOX 302/404 library has all SEC Final Rules and all "clarifications" and PCAOB AS#2 and all "clarifications".	• Invest the time and internal resources to stay on top of all of the changes or seek outside professional advice.

parson consulting

PAISLEY CONSULTING

Business accountability solutions.

SOX Cost Reduction Strategies

Issue	Action
• Utilize SOX 302/404 software that supports TOP-DOWN/RISK-BASED assessment methods.	• Invest in SOX compliance software for sustainability, controls optimization, and lower costs. Your SOX solution should embrace both the existing bottoms up and future top-down risk based processes.

parson consulting

©2006 Paisley Consulting. All Rights Reserved

PAISLEY CONSULTING

Business accountability solutions.

SOX Cost Reduction Strategies

Issue	Action
• Although the SOX assessment rules are in transition, significant savings are available to companies that know what the SEC requires and have the right advice, training and technology.	• Invest the time and internal resource to become experts on the topic or seek the assistance of outside professionals.

parson consulting

PAISLEY CONSULTING

Business accountability solutions.

Q&A

parson consulting

PAISLEY CONSULTING

Business accountability solutions.

More Information

- Visit our websites:
  - www.paisleyconsulting.com
  - www.parsonconsulting.com
- For more questions, contact Tim Leech
  - tim.leech@paisleyconsulting.com

parson consulting