

Auditing Standard 5- Effective and Efficient SOX Compliance

September 6, 2007

Presented to: The Dallas Chapter of the Institute of Internal Auditors

Today's Agenda

- Where have we been - ***Background & Summary of SEC and PCAOB guidance***
- Where are we now
- Where should we be headed - ***Opportunity for Change***
- Management's Framework for Change
- Moving toward Optimization

Where have we been....

History of Section 404

July 2002

Sarbanes-Oxley Act proposed

July 2003

Final rules adopted for Sarbanes-Oxley Section 404

March 2004

Accounting Standard 2 adopted

May 2005

Guidance released by PCAOB

Dec 2006

Proposed SEC Interpretive Guidance for Management and proposed Accounting Standard 5 released

May 2007

SEC Approval of Guidance for Management & PCAOB Approval of AS5

Where Have We Been?

- Highly prescriptive approach
- Too many key controls identified
- Extensive time and effort- management and auditors
- Numerous exceptions-mostly below “significant” threshold
- Inconsistent reliance on automated controls
- Lack of reliance on direct entity level controls
- Ongoing remediation efforts...
- ..and most of all..

Costs have been high...

...but trend is positive

- To evaluate SOX compliance cost trends, the Big 4 commissioned a survey by CRA International, which compared SOX compliance cost information for accelerated filers in Years 2 and 3
- Costs declined year over year for both large and small filers

Category	Year 1 Costs* (000's)	Year 2 Costs* (000's)	Percent Change*
Large Filers	\$8,510	\$4,770	-43.9%
Small Filers	\$1,241	860	-30.7%



Alignment of SEC guidance for management and PCAOB guidance for auditors

- **Efficiency** - Rules have been designed to drive more efficiency while maintaining the effectiveness of the evaluation of internal control over financial reporting (ICFR)
- **ICFR Evaluation** - Rules allow an opportunity to modify a registrant's ICFR evaluation methodology
- **Roadmap for Auditors** - Rules also create an opportunity for management to develop an approach to 404 compliance that offers a more efficient roadmap for their auditors
- **Cost Reduction** - Rules will likely allow a reduction in internal compliance costs for registrants and may provide an opportunity for a more efficient approach to be undertaken by a registrant's auditors

SEC Guidance

- **Principles based.** Allows for management to exercise significant judgment versus AS2 specifics
- **Non-prescriptive.** Does not provide a checklist of steps for management to perform in completing its evaluation
- **Top-down, Risk-based Approach.** Encourages management to focus only on those controls that are needed to adequately address the risk of a material misstatement in its financial statements
- **Scalable.** Enables companies to scale and tailor their evaluation methods and procedures to fit their own facts and circumstances
- **Not Absolute.** Recognizes internal controls cannot prevent/detect all misstatements and also allows for management to base its decisions upon the full range of appropriate conduct, conclusions, and methodologies
- **Smaller Companies.** Potentially has greatest impact on smaller companies and those in the early stages of implementation

PCAOB - AS5

- Eliminates the requirement for auditors to opine on **management's assessment process**
- Auditors should focus on most important key controls upon a **top down, risk-based evaluation**
- Emphasizes consideration of **entity level controls**
- Permits consideration of **knowledge obtained during previous audits** which may allow reduced testing of units in scope
- Refocuses the **multi-location testing** requirements on risk rather than coverage
- Redefines significant **deficiency and material weakness** and introduces the concept of “reasonably possible” versus “remote”
- Provides for increasing the reliance on the **work of others** in conducting the audit
- Recalibrates the **walkthrough requirements**, focusing on significant processes

Where we should be headed

Opportunity for Change...

- Registrants have an opportunity to **take the lead in defining their overall control environment** and the approach they will use in maintaining and evaluating the effectiveness of ICFR
- Management also has an opportunity to demonstrate to their auditor a **more efficient methodology** for meeting their annual 404 audit requirement by **providing the auditor with a roadmap** of their top down, risk-based evaluation approach while at the same time meeting the SEC's documentation expectations
- The SEC's principles based guidance, along with a top down, risk-based approach provides management with **significant latitude in defining the annual assessment process** – e.g., detailed testing of direct entity level controls and a more limited number of critical process level key controls in combination with a self assessment approach for non critical key process level controls

AS5-Effective and Efficient SOx Compliance

The most significant difference between the approaches is the timing and level of the overall risk assessment and more robust reliance on direct entity level controls (ELC).

Prior Approach

- Analyze financial statements
- Identify significant locations based on revenue, assets
- Identify key accounts
- Identify the processes related to key accounts by location
- Document the processes
- Identify financial reporting risks inherent in business processes
- Identify controls that mitigate the identified risks
- Test all controls every year
- Materiality focused at significant deficiency level



Updated Approach

- Analyze financial statements
- Identify significant accounts
- Identify entity level controls that address risks (direct ELC)
- Materiality focused at material weakness level using qualitative characteristics
- Focuses on contribution of ELCs to reduce critical key controls for testing
- Determine residual financial reporting risk
- Identify critical process level key controls to mitigate residual risk
- Develop tests for all entity level and critical process level key controls
- Test ELC and critical process level key controls
- Monitor other key controls through walkthroughs, self assessments or internal audits

The updated approach requires an understanding of the following concepts:

Direct Entity Level Controls (ELC) – ELCs that are designed to identify potential financial reporting errors for timely correction are considered direct entity level controls (e.g., management analytics)

Indirect Entity Level Controls – ELCs that provide impact on the overall control environment (e.g., Code of Conduct)

Critical Process Level Key Controls – Process level key controls that are designed to address specific residual financial reporting risks after consideration of direct ELCs

Management's Framework for Change

Management's framework for change

- Two important principles to management's evaluation process:
 - **Management should** evaluate the design of controls **to determine whether there is a reasonable possibility that a material misstatement in the financial statements would not be prevented or detected.**
 - **Management should** gather and analyze evidence **about the operation of the controls being evaluated** based on its assessment of the risk **associated with those controls**

The new guidance does not require management to make changes, but for many organizations there is likely to be opportunity for improved effectiveness and efficiency in management's evaluation process.

Management's framework for change

Management's Risk Assessment Process

- Focus on identifying those risks that may result in a material misstatement of the financial statements
- **Obtain input regarding risk** exposures from various sources (e.g., audit committee, controller, internal audit, disclosure committee, SEC comments)
- Establish procedures for **monitoring changes** in risk throughout the year
- Consider other areas where a more **concerted “top down” focus** might drive better efficiency (e.g., segregation of duties; reconciliations)
- Refocus multi-location testing requirements on **coverage of risk**, rather than coverage of balance sheet/ statement of earnings
- Enhance process to facilitate top down risk assessment

Management's framework for change

Re-assess effectiveness of Entity Level Controls

- Evaluate the relationship of the ELCs to the financial statement accounts (i.e., determine if the relationship is direct [e.g., robust management analytics] or indirect [e.g., tone at the top])
- For example, ensure management analytics, a direct ELC, is performed at a level of precision to detect potential material misstatements (e.g., detailed analysis such as gross margin by product line, days sales outstanding, etc.)
- Determine if key individuals possess the appropriate skills and have the competencies to execute the ELCs

Management's framework for change

Re-assess effectiveness of Entity Level Controls (continued)

- Link process level key controls to residual risks identified during the risk assessment
- Take **credit for controls** that mitigate risk in more than one financial statement line item
- Identify ITGCs that may help ensure effectiveness of automated controls
- Challenge the business processes considered during key control identification - **only test the controls that are important to preventing or detecting material misstatements of the financial statements**

Re-focus on Information Technology Controls

- It is important to distinguish among IT controls that are designed to address **financial reporting** risks and those that exist to meet operational objectives or to ensure compliance with laws and regulations.

- **The risks that are likely to be important to most auditors:**
 - **Security:** Restrict unauthorized access to programs and data
 - Ensure **Program Changes** (including changes to financial controls and reports) are authorized, correctly defined, tested and properly implemented
 - SDLC or **Program Development** impacting financial systems or data.
 - Computer operations related to specific risks such of job scheduling, batch processing or interface management **Impacting Financial Data.**

Management's framework for change

AS5 impact – Focusing on financial reporting risks

Almost Always Relevant	Access to Programs and Data <ul style="list-style-type: none">▪ Application and data security▪ Control of powerful access▪ User provisioning and SOD management	Program Change Control <ul style="list-style-type: none">▪ Change requirements and business approval▪ Testing▪ Authorization to production▪ Control of promote to production process
Varying Relevance	Program Development <ul style="list-style-type: none">▪ System Design▪ Interfaces and Data Conversion▪ Automated Controls▪ Testing▪ Go Live Approvals	Computer Operations <ul style="list-style-type: none">▪ Batch job and interface control and monitoring▪ Backups and data recovery▪ Infrastructure Changes

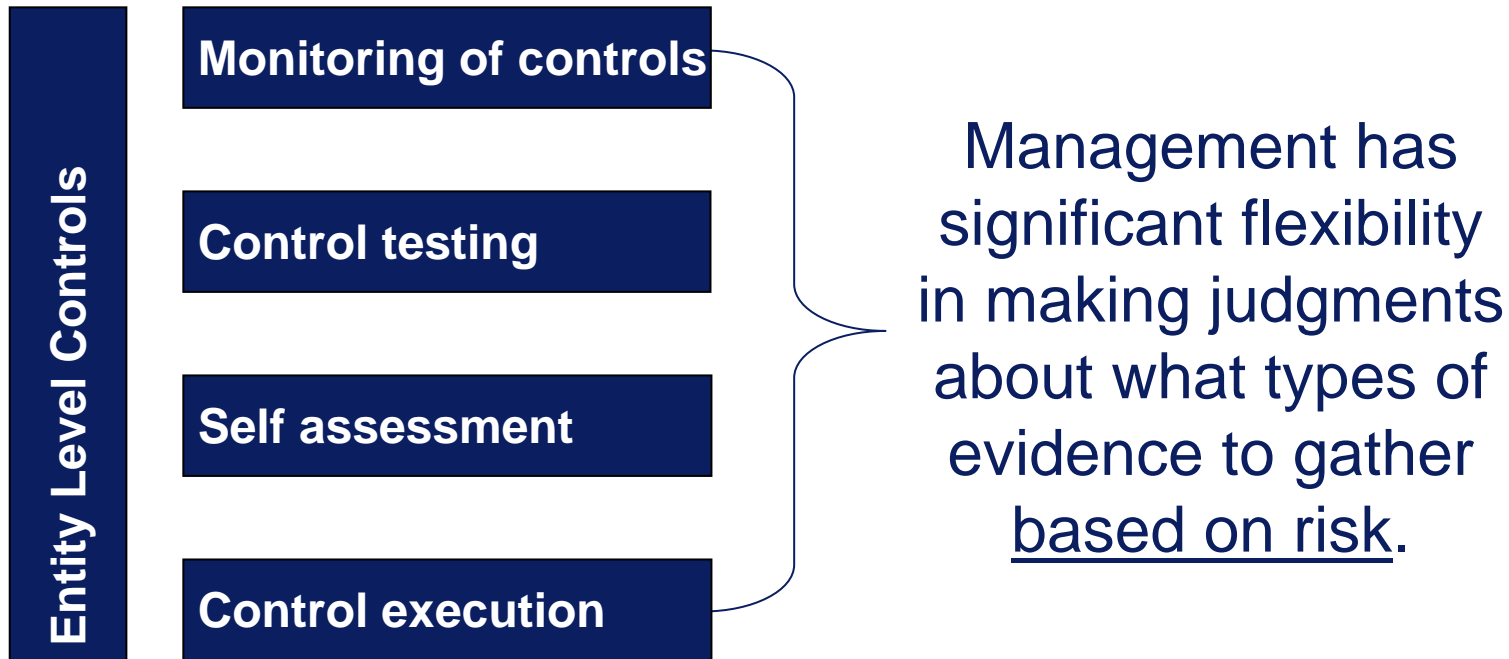
Management's framework for change

Testing operating effectiveness

- Vary the nature, timing and extent of the methods based on both:
 - The risk of control failure
 - The risk of material misstatement
- Consider the **persuasiveness of the evidence** needed (i.e., its qualitative characteristics, not just the quantity)
- Use the same risk-based approach and consideration for testing IT general controls; vary the nature, timing and extent of methods accordingly

Management's framework for change

Testing operating effectiveness - strategies



One would generally expect more efficient approaches (such as self-assessment) in low-risk areas, and more extensive testing in high risk areas.

Management's framework for change

Using the work of others

- Extent of reliance by the auditor on the work of others depends on:
 - Competency and objectivity of those performing the testing
 - Nature (complexity and risk) of subject matter to be tested by others
- Potential for increased reliance on the work of others in areas such as:
 - Certain aspects of the control environment
 - Direct assistance with walkthroughs

Management's framework for change

Develop a Sustainable Program

- **Formalize a sustainability program** that ensures ICFR in all business processes are designed properly and operating effectively throughout each year- allowing for comfort that direct ELCs and critical process level key controls can stand up to the risks of a material misstatement in the financial statements
- **Implement an operating structure** that ensures that changes impacting process level controls result in timely updates to control documentation and effectiveness re-evaluation
- Ensure **self assessments** of process level controls are performed and documented routinely
- Institute an **accountability structure** where line management are held accountable for the ICFR sustainable operational structure
- Establish mechanisms to **challenge the effectiveness** of self assessments

Develop and implement a more robust and thorough sustainability program over ICFR.

The rules can result in changes to the methodology for evaluating the effectiveness of ICFR and may create efficiencies such as:

- Fewer key controls in scope
- Fewer full scope locations
- Increased use of judgment based testing
- Information Technology General Controls (ITGC) may allow for the spreading of automated control testing over several periods
- Improvements to overall corporate governance resulting from strengthening ELCs

In summary.... Where should you be in the process

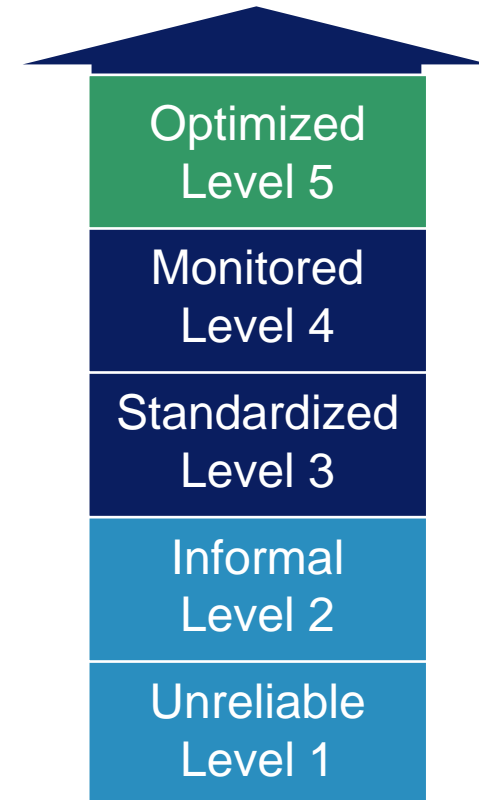
- **For the 12/31 year ends, you should have completed the following steps :**
 - Completed the risk assessment
 - Determined which ELCs to leverage this year
 - Analyzed scope relative to risks
 - Re-assessed inventory of key controls
 - Discussed current-year scope, testing approach and auditor reliance with external auditors and obtained consensus
 - Management and external auditor testing should be underway

The Path Forward – Moving toward Optimization

Controls optimization

There are several ways to optimize SOX controls:

- **Reduce** complexity (both process and controls)
- **Integrate** Governance, Risk and Compliance (iGRC)
- **Shift** from reactive to proactive/from detective to preventive
- **Leverage Technology**
 - Use technology to support Governance, Risk and Compliance
 - Automate manual controls and controls assurance/leverage controls functionality in your environment (at all levels of the infrastructure):
 - Spreadsheet optimization
 - Identity Management
 - ERP



Reduce complexity- use a top-down risk based approach to identify the “right” controls for the business

- **Approach it strategically** – understand the broader organization objectives beyond the current, targeted governance, compliance and risk focus
- **Drive change** by anchoring in a common set of risk and compliance principles
 - **Optimize the design** of controls
 - Standardize and centralize disparate control activities
 - Maximize opportunities to replace manual controls with automated controls
 - **Embed compliance and controls** within processes and technology

Enhanced efficiency and effectiveness leads to Controls Optimization

Improve efficiency

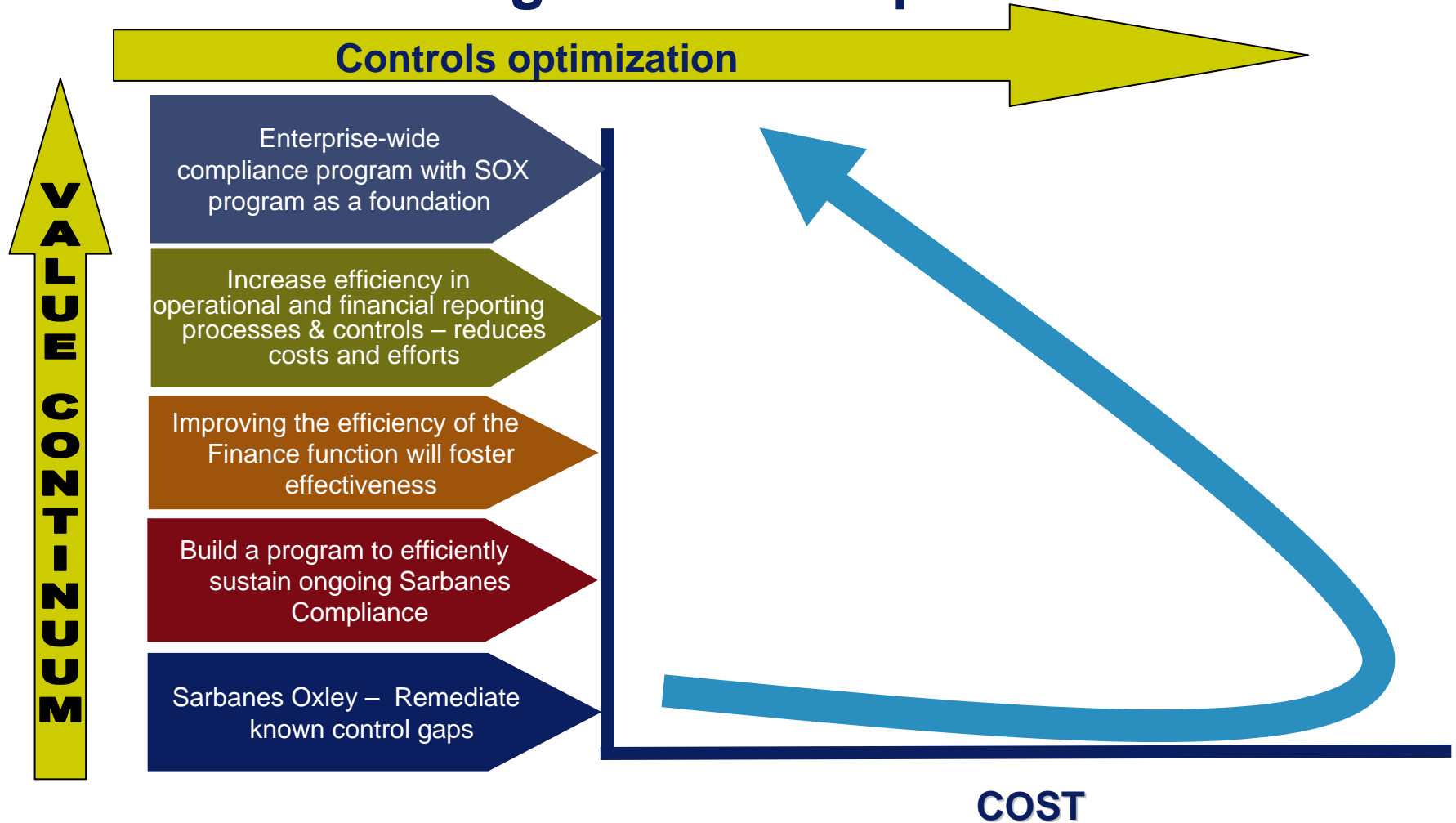
- Minimize duplication of effort
- Reallocate business unit resources back to revenue generation
- Control the growth in GRC related expenses
- Align timelines
- Manage your response to the regulatory environment, not just react to it
- Establish an extensible operating model that can handle the “next big initiative”

Improve effectiveness

- Minimize unidentified risks by executing a comprehensive evaluation process
- Improve the content, quality and timing of analysis and reporting
- Readily explain operating model to third parties

Where are we going?

The Path to Driving Value via Optimization



Questions?

Contact information

Phil Samson, Partner

(214) 754-7269

Phil.Samson@us.pwc.com

Chris Williams, Partner

(214) 756-1645

Christopher.M.Williams@us.pwc.com

Maanasa Jain, Senior Manager

(214) 754-5313

Maanasa.Jain@us.pwc.com

Colby Ton, Senior Manager

(214) 981-7144

Colby.G.Ton@us.pwc.com



This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers LLP, its members, employees and agents accept no liability, and disclaim all responsibility, for the consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2007 PricewaterhouseCoopers LLP. All rights reserved. "PricewaterhouseCoopers" refers to PricewaterhouseCoopers LLP (a Delaware limited liability partnership) or, as the context requires, other member firms of PricewaterhouseCoopers International Ltd., each of which is a separate and independent legal entity. *connectedthinking is a trademark of PricewaterhouseCoopers LLP.