Sarbanes-Oxley (US-SOX)

Ken Vander Wal, Retired
Ernst & Young, LLP
Chicago, Illinois, USA
vandeke@gmail.com

Agenda Topics

- History of SOX Legislation
- Evaluating Deficiencies
- IT Lessons From Year 1
- SOX Opportunities
- Questions
- Appendix: Other SOX Guidance

History of SOX Legislation

Historical Timeline

July 30, 2002	Sarbanes-Oxley Bill Signed by Bush
August 29, 2002	302 Quarterly Filing in Effect
Q4, 2002	PCAOB Formed
June 5, 2003	Final 404 Rules Issued by the SEC
October 7, 2003	PCAOB Issues Draft of AS/2
June 17, 2004	SEC Approves AS/2
May 16, 2005	Guidance Issued for Top-Down Risk-Based Approach

Historical Timeline (cont.)

December 19, 2006	PCAOB Issues Draft of AS/5 as a Replacement for AS/2
December 20, 2006	SEC Issues Proposed Interpretative Guidance for Management
May 23, 2007	SEC Approved Final Interpretive Guidance for Management
May 24, 2007	PCAOB Voted to Adopt AS/5
July 25, 2007	SEC Approved AS/5

Deferral of 404 for US Issuers

Accelerated Filer Status	Management's Report	Auditor's Attestation
Large Accelerated Filer OR Accelerated Filer ($75M or >)	Already Complying (since November 15, 2004)	Already Complying
Non-accelerated Filer (<$75M)	Annual Reports for Fiscal Years Ending on or after 12/15/2007	Annual Reports for Fiscal Years Ending on or after 12/15/2009

Deferral of 404 for Foreign Issuers

Accelerated Filer Status	Management's Report	Auditor's Attestation
Large Accelerated Filer (700M or >)	Annual Reports for Fiscal Years Ending on or after 7/15/2006	Annual Reports for Fiscal Years Ending on or after 7/15/2006
Accelerated Filer (> or =$75M and < $700M)	Annual Reports for Fiscal Years Ending on or after 7/15/2006	Annual Reports for Fiscal Years Ending on or after 7/15/2007
Non-accelerated Filer (< $75M)	Annual Reports for Fiscal Years Ending on or after 12/15/2007	Annual Reports for Fiscal Years Ending on or after 12/15/2009
Newly Public Company (US or Foreign Issuers)	Second Annual Report	Second Annual Report

Evaluating Deficiencies

Guidance on Evaluating Deficiencies

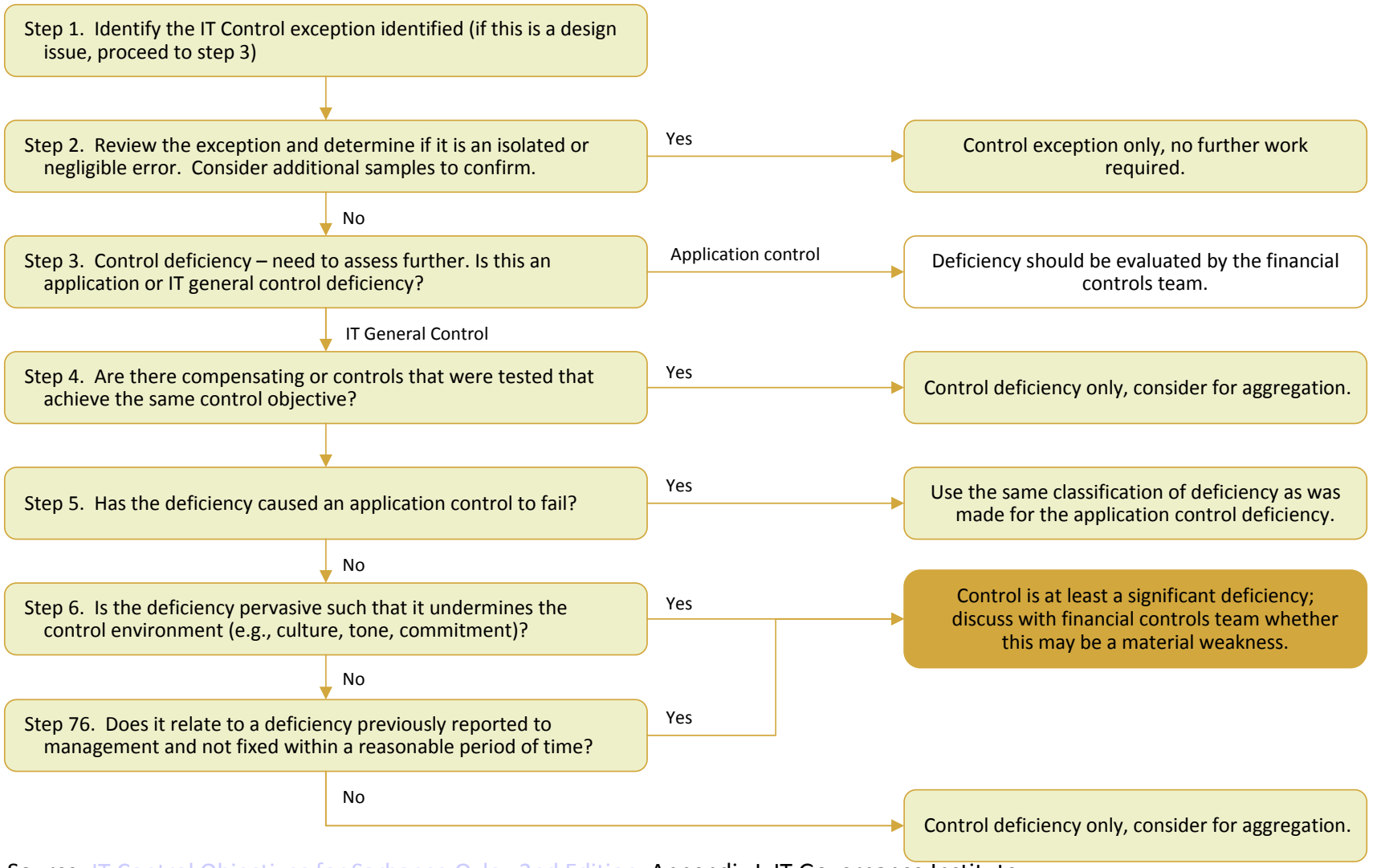
- ITGI Guidance
  - ❖ Considers Both Control Design and Effectiveness
  - ❖ Included in Publication IT Control Objectives for Sarbanes Oxley 2nd Edition
    - A Framework for Evaluating Control Exceptions and Deficiencies, Version 3, December 20, 2004
  - ❖ Developed by Representatives of Nine US Public Accounting Firms and University Professor
  - ❖ Served as Guidance During Initial Years of SOX
  - ❖ Never Became “Official-endorsed” Guidance

Compliance Trends SOX Issue
Prevalence by Internal Control Issue

			Internal Control Issues					
	404 Opinions Filed	404 Opinions with Material Weaknesses as of 8-11-07	Person-nel Issues	Segrega-tion of Duties	Restate-ments of Financials	Material YE Adjust-ments	Internal Audit Issues	IT Processing, Access Issues
2006	4051	348 (8.6%)	165 (47.4%)	53 (15.2%)	91 (26.1%)	233 (67.0%)	9 (2.6%)	65 (18.7%)
2005	3791	390 (10.3%)	207 (53.1%)	57 (14.6%)	177 (45.4%)	250 (64.1%)	4 (1.0%)	79 (20.3%)
2004	3700	624 (16.9%)	304 (48.7%)	149 (23.9%)	324 (51.9%)	335 (53.7%)	17 (2.7%)	135 (21.6%)

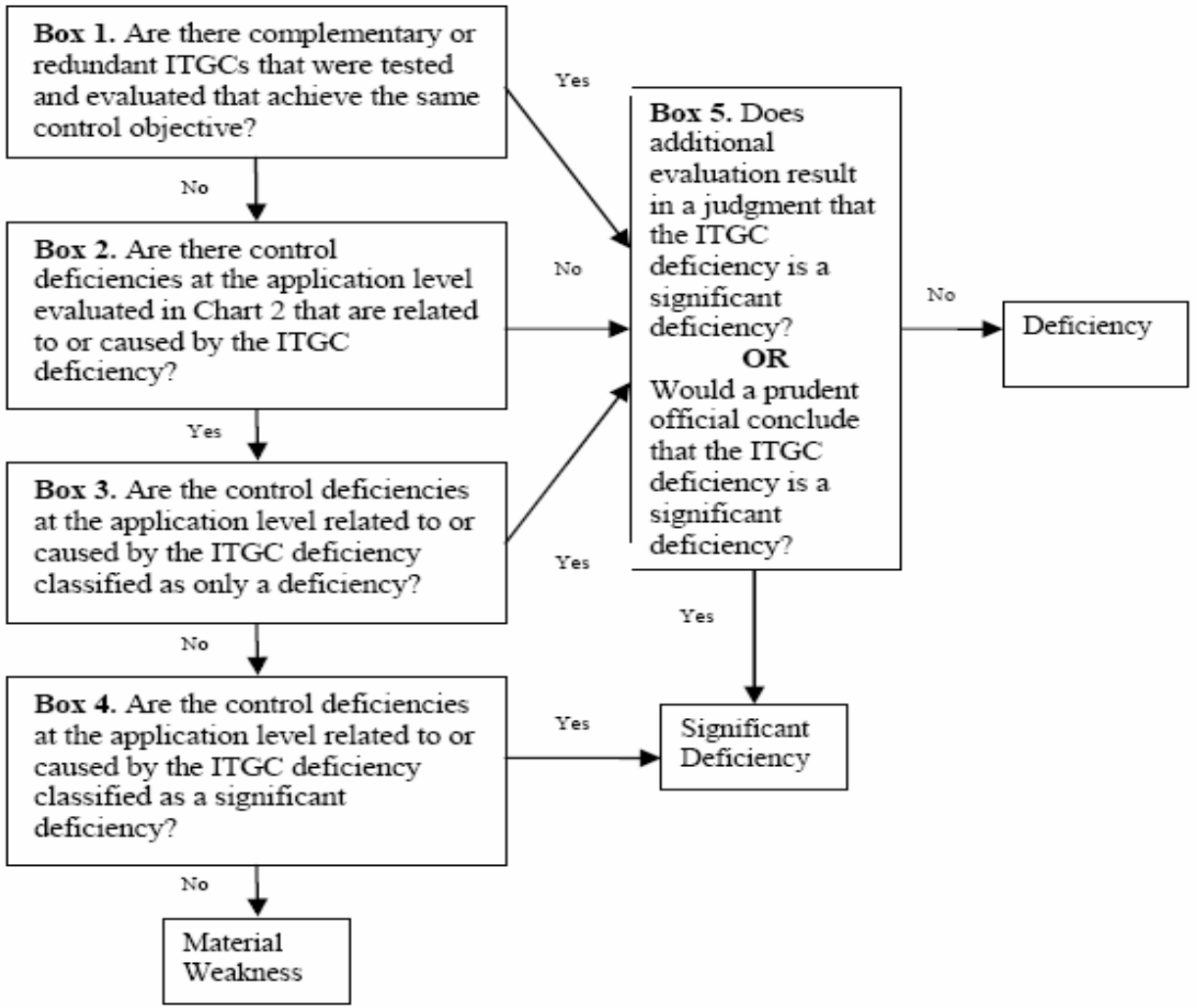
* Source: Audit Analytics ® 404 Dashboard Year 3 Update, December 2007

ITGI Guidance



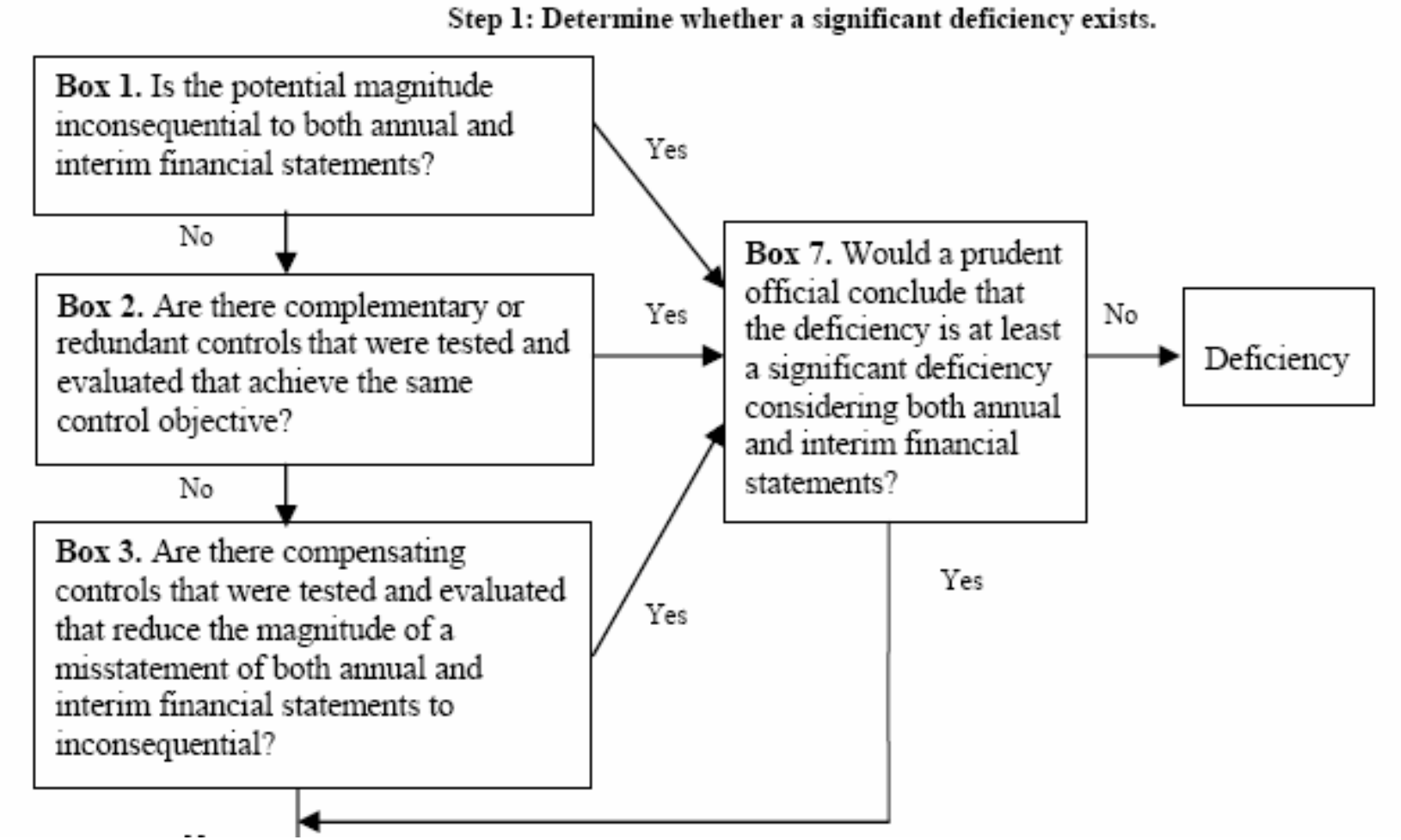
Source: IT Control Objectives for Sarbanes-Oxley 2nd Edition, Appendix I, IT Governance Institute

Evaluating Information Technology General Control (ITGC) Deficiencies



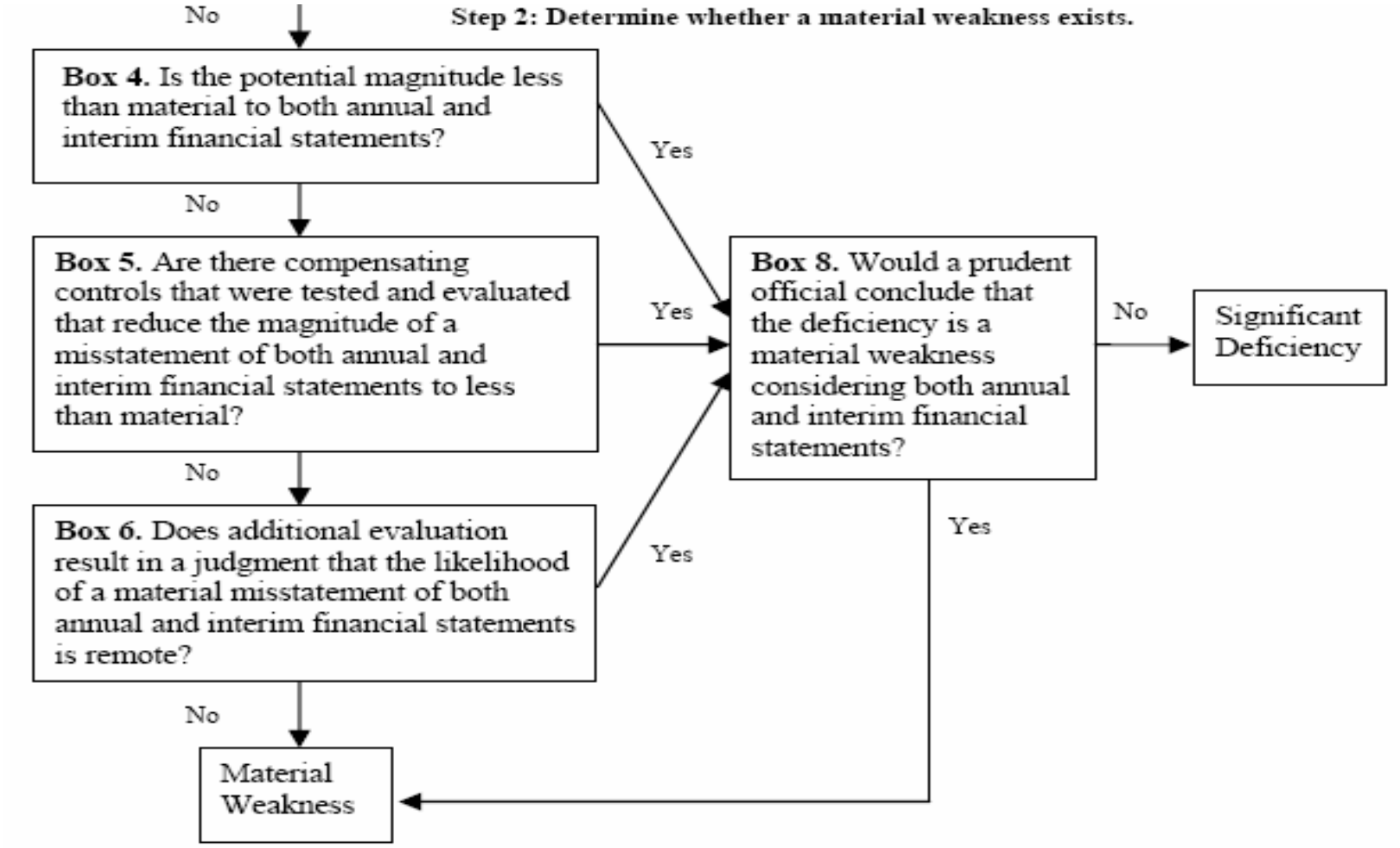
Source: A Framework for Evaluating Control Exceptions and Deficiencies, Version 3, December 20, 2004

Evaluating Process/Transaction-Level Control Deficiencies



Source: A Framework for Evaluating Control Exceptions and Deficiencies, Version 3, December 20, 2004

Evaluating Process/Transaction-Level Control Deficiencies (continued)



Source: A Framework for Evaluating Control Exceptions and Deficiencies, Version 3, December 20, 2004

IT Lessons From Year 1

Lessons From Year 1
(From an IT Perspective)

- Too Many Applications Included in Scope
- Focused on General Controls Before Application-Level Controls
- IT Review and Assessment Not Integrated Into Overall SOX Project
- Failure to Focus on “KEY” IT Controls
- Detective Controls Implemented in Year 1 to Compensate for Ineffective IT Controls

Lessons From Year 1 (continued)
(From an IT Perspective)

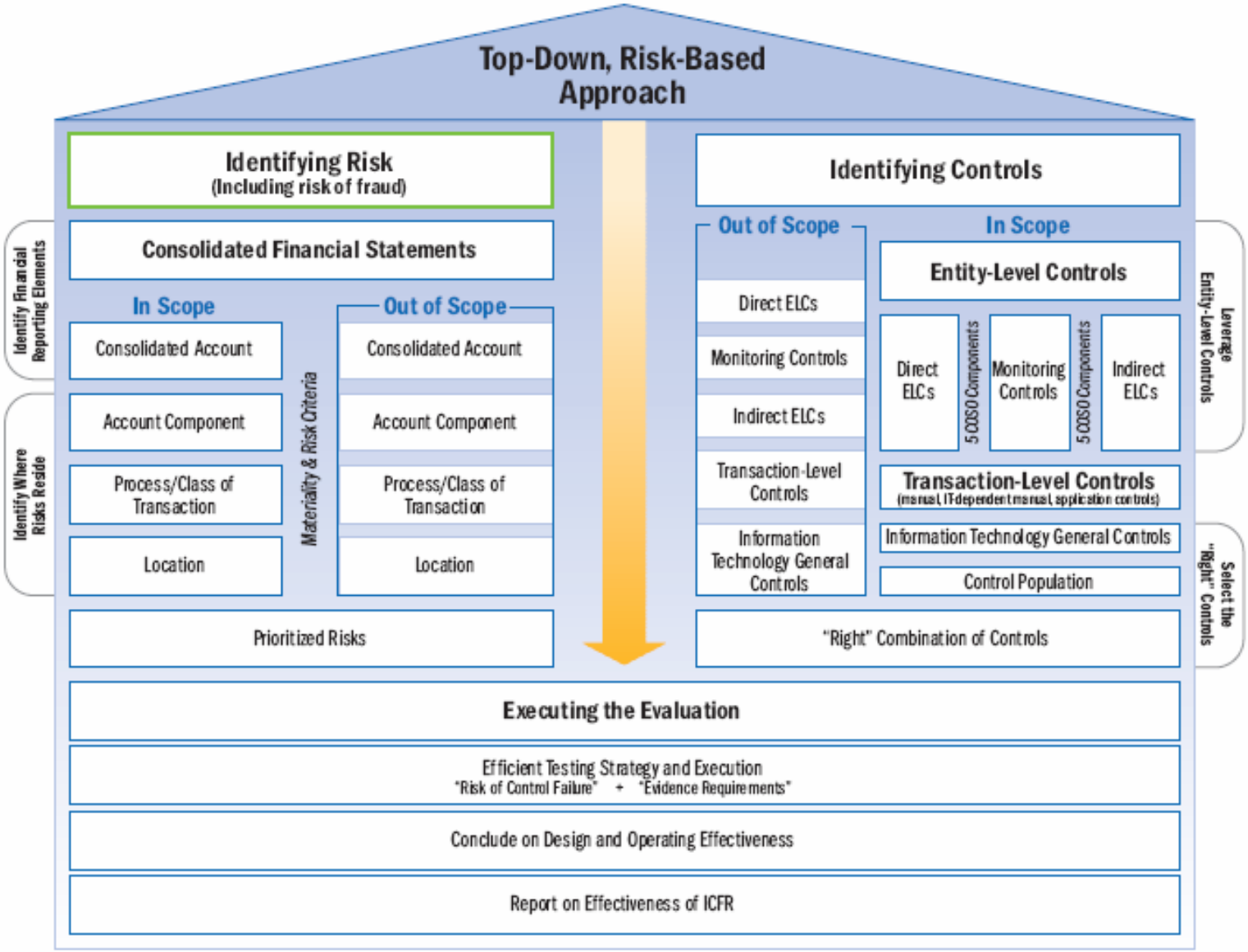
- Need for More Ownership by Business Units Over Documentation and Testing of Applications
- More Efficient to Document and Test Centralized Processes and Operations
- Need to Address SOX as a Process versus a One-Time Project

SOX Opportunities

Three Higher-Level SOX Opportunities

- Applying A Top-Down, Risk-Based Approach
- Leveraging Entity Level/Monitoring Controls
- Maximizing Your SOX Investment

There Are Many Other Opportunities



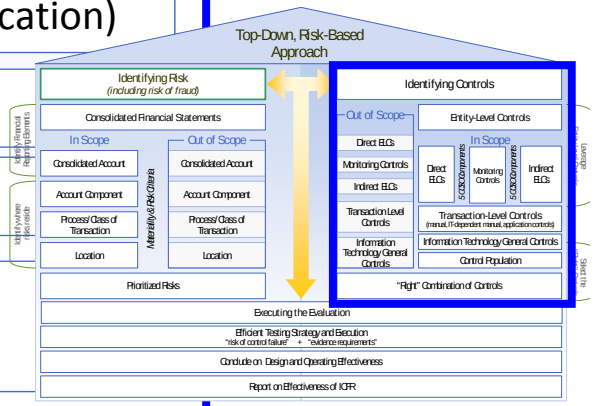
Source: The New 404 Balancing Act, Ernst & Young, 2007

Identifying and Evaluating Controls

Identifying Controls

Out of Scope	In Scope
Direct ELCs	Entity-Level Controls (ELCs)
Monitoring Controls	Direct ELCs; Monitoring Controls; Indirect ELCs
Indirect ELCs	
Transaction Level Controls	Transaction-Level Controls (manual, IT-dependent manual, application)
Information Technology General Controls	IT General Controls
	Control Population

“Right” Combination of Controls



Efficiency Opportunities in Control Identification

- Identify ELCs early in the scoping process and leverage throughout
- Focus on whether controls address identified risks, not their “label”
- Strive for “right” combination of controls
- Heavily leverage effective IT controls

Applying Top-Down, Risk-Based Approach to IT Controls

- There generally is a correlation between the risk related to IT general controls and the underlying application or IT-dependent manual controls
- The risk associated with IT general controls is heavily influenced by the pervasiveness across multiple platforms or applications
- The nature, timing, and extent of IT general control testing should correlate with the risk within the IT environment
- There is no requirement to test IT general controls if no reliance is being placed on application or IT-dependent manual controls

Efficiency Opportunities for IT Controls

- Increase the percentage of automated controls
- Increase the number of common IT general controls by standardizing, centralizing, and consolidating IT processes
- Test common controls across platforms as one population versus multiple populations
- Leverage the use of Benchmarking as applied to automated controls
- Explore the benefits posed from the use of Continuous Controls Monitoring tools

Example of IT Top-Down, Risk-Based Approach

Scenario

- Multi-division company, but application used only at 1 in-scope division
- Application complexity:
  - AS 400, non-web based, several hundred users, supports only one process (e.g., inventory)
  - Source code is present and developers make changes
- Process in question has numerous key manual detect controls, but only a few application or IT-dependent controls

Proposed Example Applying the Risk-Based Approach

- Walk through IT General Controls
- Manage Changes
  - Tested programmer separation from production
  - No testing of program changes beyond walk-through since risk-based approach determined relevant application controls were more dependent on logical access than program changes
- Logical Access
  - Tested sample of current users for segregation of duties
  - Tested super-users at operating system and database levels
  - AS/400 configuration settings verified as part of walk-through – no more testing required
  - No further database testing

Leveraging Entity-Level Controls

- The SEC guidance highlights three kinds of ELCs:
  - Important, but indirect effect
  - Identify possible breakdowns in lower level controls
  - Directly address risk of misstatement
- When entity level controls are linked, fewer number of transaction level controls may be needed
- Having direct entity level controls as part of the combination of controls reduces the level of evidence needed from transaction level controls
- Direct entity level controls, including monitoring controls, can often be leveraged to reduce testing in low risk areas

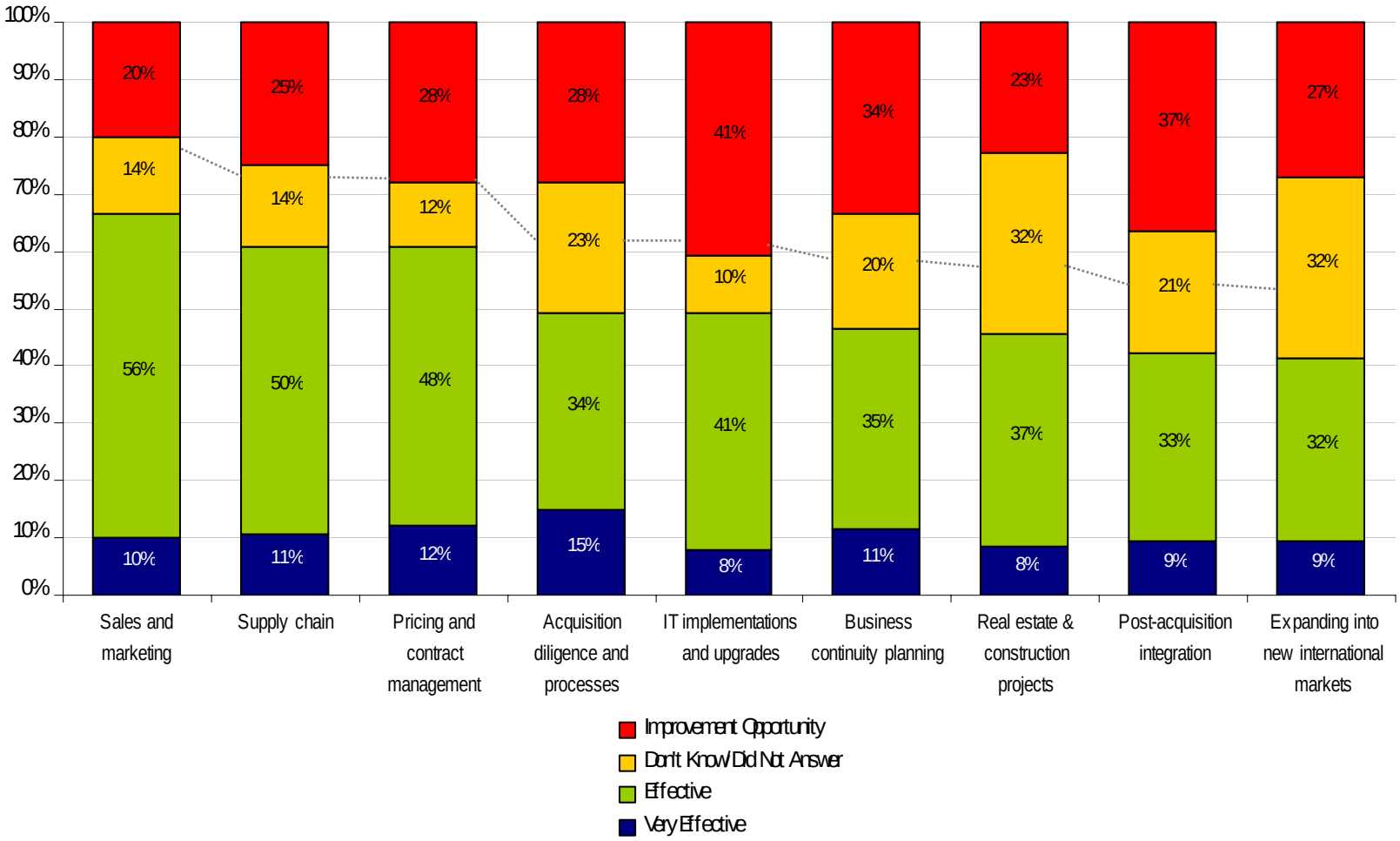
Entity Level Controls and IT

- Same leverage when applied to IT
- May already be covered by existing testing of ELCs
- Examples of IT-related ELCs
  - IT Organization and Relationship (Segregation of Duties)
  - IT Policies and Procedures
  - IT Risk Assessment Plan
  - IT Management of Human Resources
  - Training and Education

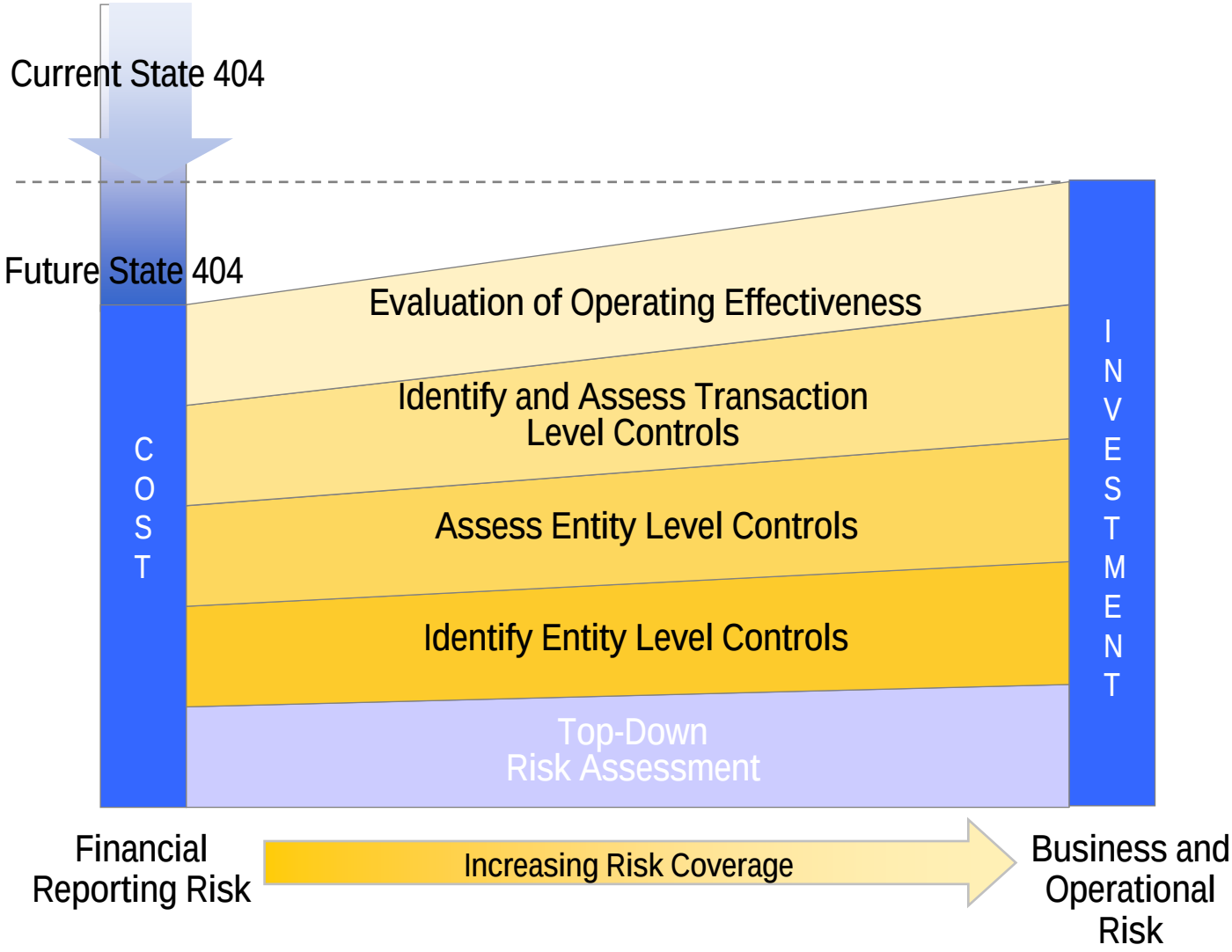
Maximizing SOX Investments

2007 E&Y Survey

How effective are internal controls over the following business and operational areas?



Leveraging Internal Control Investment



SOX Self-Assessment Tool

		Transformation	Transition	Leading Practice
Transformation	1. What criteria have you used to determine sufficiency of evidence?	AS5	Peer Analysis	SEC Guidance
	2. How has the organization structured its resources to manage the 404 program effort?	No PMO/Ad-Hoc	Project	Program
	3. How comfortable are you that your current 404 approach incorporates the necessary skills and knowledge to implement a top-down, risk-based approach?	Uncomfortable	Somewhat Comfortable	Very Comfortable
	4. How would you assess the efficiency of your company's existing 404 processes?	Inefficient	Somewhat Efficient	Efficient
Top-Down, Risk-Based Approach	5. What was your starting point in preparing the risk assessment?	Locations	Controls	Risks
	6. What level of documentation did you develop and maintain for your 404 program efforts?	Exhaustive	Excessive	Efficient
	7. What was the main factor driving your testing strategy?	Coverage	Control	Risk
	8. To what extent have you leveraged shared services or other centralized processing?	No Leverage	Some Leverage	Full Leverage
Entity Level Controls	9. At what point in your process have you identified and evaluated ELCs?	End of Process	Middle of Process	Beginning of Process
	10. To what degree have you leveraged your direct ELCs?	No Leverage	Some Leverage	Full Leverage
IT Controls	11. Has the company effectively leveraged the use of application controls within the overall control population?	Ineffective	Effective	Highly Effective
	12. How efficiently has the company employed a top-down, risk-based approach to identifying and testing ITGCs?	Inefficient	Somewhat Efficient	Efficient

Source: The New 404 Balancing Act, Ernst & Young, 2007

THANK YOU

Appendix:
Additional SOX Guidance

- PCAOB Guidance for Auditors of Smaller Public Companies
- COSO[1] Guidance on Smaller Public Companies
- COSO Guidance on Monitoring Internal Control Systems

[1] COSO: Committee of Sponsoring Organizations (www.coso.org)

•PCAOB Guidance for Auditors of Smaller Public Companies

- Issued for comment on October 17, 2007
- Available: http://www.pcaobus.org/news_and_events/news/2007/10-17.aspx
- Objective: Help auditors understand the types of controls that might be encountered in the audit of a smaller, less complex company and to provide a context for discussion of audit strategies for evaluating the effectiveness of those controls
- Attributes of a smaller, less complex company
  - ❖ Use of entity-level controls to achieve control objectives
  - ❖ Risk of management override
  - ❖ Implementation of segregation of duties and alternative controls
  - ❖ Use of information technology
  - ❖ Maintenance of financial reporting competencies
  - ❖ Nature and extent of documentation

PCAOB Guidance for Auditors of Smaller Public Companies-Chapter 5

- Auditing IT controls in a less complex IT environment
- Characteristics of less complex IT environments
  - ❖Tendency to rely on manual controls over transaction processing
  - ❖Use of off-the-shelf software
  - ❖Centralized computer systems
  - ❖More dependency on end-user computing

COSO Guidance on Smaller Public Companies

- Issued June 2006
- 4 Volumes
  1) High-level summary for companies' boards of directors and senior management
  2) Overview of internal control over financial reporting in smaller businesses
  3) Illustrative tools to assist management in evaluating internal control
  4) Illustrative tools in Microsoft® Word format

COSO Guidance on Monitoring Internal Control Systems

- Initially Issued a discussion document for comment in September 2007
- Issued 3 volume document for comment in June 2008
  - ❖Volume 1 – Executive Summary – 22 pages
  - ❖Volume 2 – Main Guidance – 71 pages
  - ❖Volume 3 – Application Techniques – 117 pages

Executive Summary

Properly designed and executed monitoring:

- Provides persuasive information to the right people regarding the internal control system's effectiveness
- Identifies and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action and to management and the board as appropriate

In doing so, it facilitates the correction of control deficiencies *before* they materially affect the achievement of the organization's objectives.

Company Considerations Outlined in the Executive Summary

- Many organizations are performing effective monitoring in certain areas, but are not fully utilizing the results
- Monitoring considers how the *entire* internal control system addresses meaningful risks, not how individual control activities operate in isolation
- Monitoring works best when management approaches it proactively
- The board has important responsibilities in monitoring internal control
- Internal audit, through added skills and objectivity, can play an important role in assisting management and the board in monitoring

Company Considerations Outlined in the Executive Summary (cont)

- Organizations should follow a systematic process in determining “what” and “how” to monitor
- Judgment is required in determining both (a) the optimal approach to monitoring, and (b) the effectiveness of monitoring
- Monitoring generally includes the use of both direct and indirect information
- Monitoring can be performed using either “ongoing” monitoring activities or “separate evaluations”
- Computerized applications have undergone substantial development and can be built into, or added onto, existing computer applications, providing a high degree of continuous monitoring