



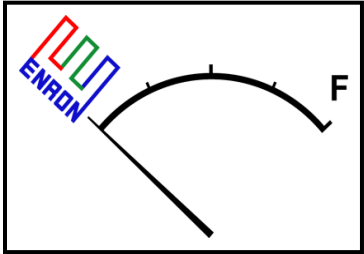
application
controls
consulting

Evaluating Your IT SOX Section 404 Compliance Program

Roxanne L. Halverson, CISM, CGEIT

Sheila Gallimore, CGEIT, CISA

The Sarbanes-Oxley Act of July 2002



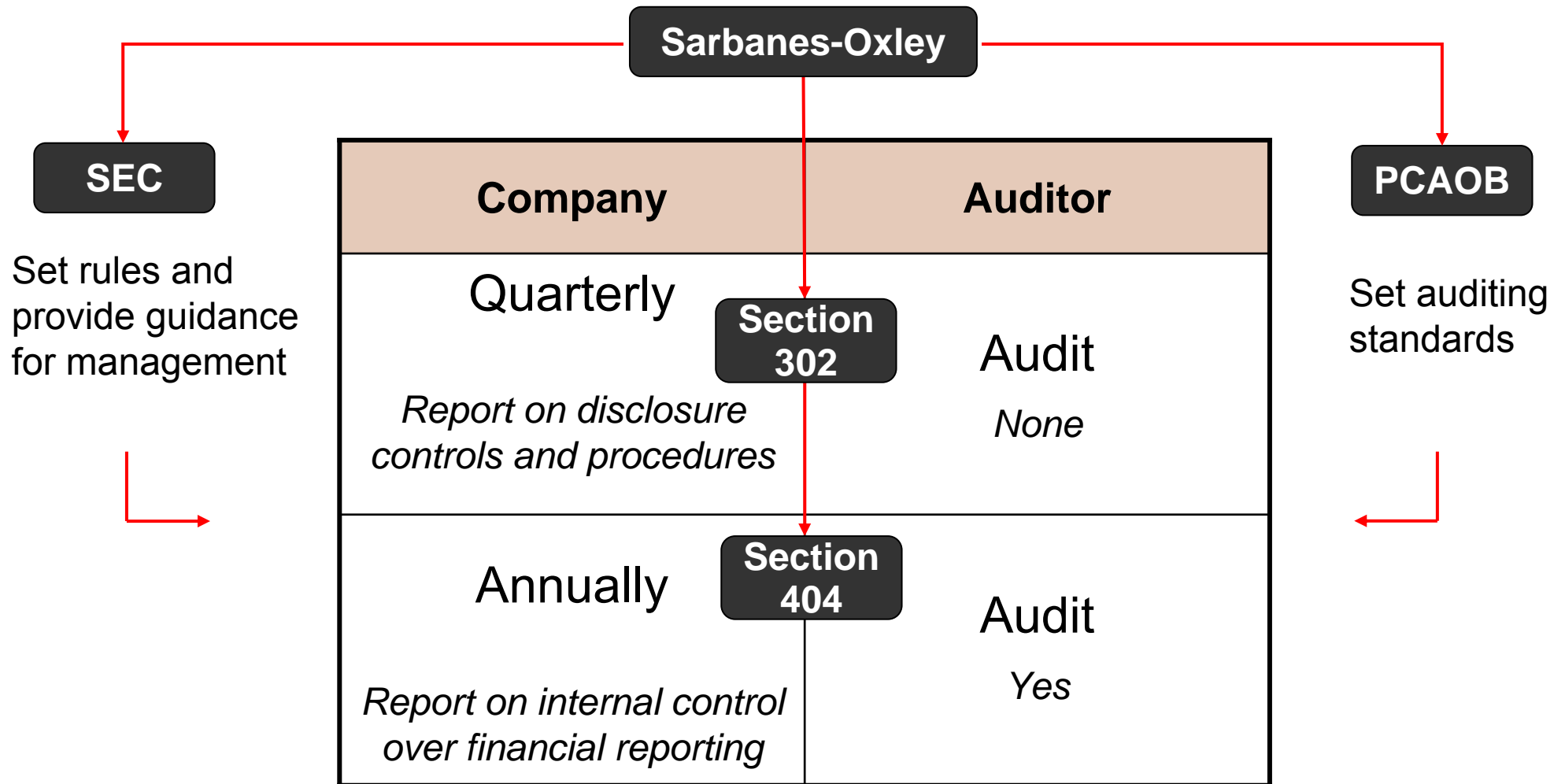
Senator
Paul Sarbanes



Representative
Michael Oxley

- Passed in the wake of a number of notable **corporate and accounting scandals** including Enron, WorldCom and Arthur Anderson.
- Required the Securities and Exchange Commission (**SEC**) to publish rules for a management assessment of Internal Controls Over Financial Reporting (**ICFR**).
- Made it clear that it is **management's responsibility** – specifically the CEO and CFO – for the adequacy of internal controls.
- Created the Public Company Accounting Oversight Board (**PCAOB**), a private-sector, non-profit corporation, to **oversee the auditors** of public companies.

Relationship of Key SOX Sections to Rules and Standards



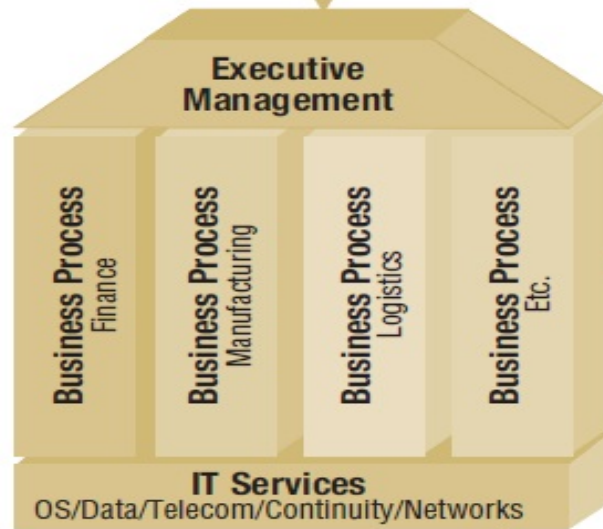
Levels of controls

Entity-level Controls

Entity-level controls set the tone and culture of the organization. IT entity-level controls are part of a company's overall control environment.

Controls include:

- Strategies and plans
- Policies and procedures
- Risk assessment activities
- Training and education
- Quality assurance
- Internal audit



Application Controls

Controls embedded within business process applications directly support financial control objectives. Such controls can be found in most financial applications including large systems such as SAP and Oracle as well as smaller OTS systems such as ACCPAC.

Control objectives/assertions include:

- Completeness
- Accuracy
- Existence/authorization
- Presentation/disclosure

IT General Controls

Controls embedded within IT processes that provide a reliable operating environment and support the effective operation of application controls

Controls include:

- Program development
- Program changes
- Access to programs and data
- Computer operations

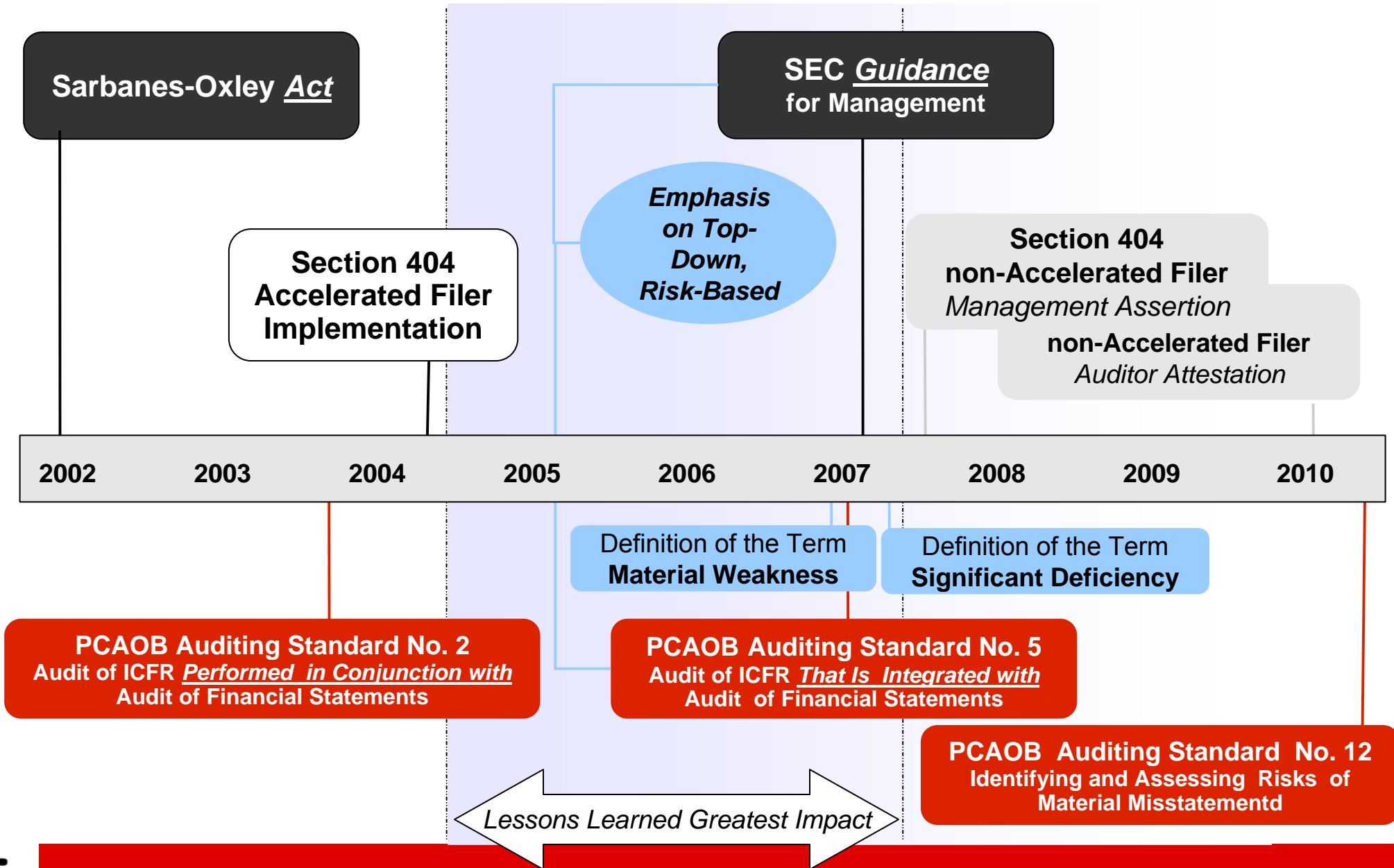


Important Term

- Key Controls
 - A control that, if it fails, means there is at least a **reasonable likelihood** that a **material error** in the financial statements would not be prevented or detected on a timely basis.
 - In other words, a key control is one that is required to provide reasonable assurance that material errors will be prevented or timely detected.
 - There is no commonly accepted definition of a key control



Major Milestones for Internal Controls Over Financial Reporting Related to IT



SEC “Final Rule” Definitions

- Material Weakness¹
 - a deficiency, or a combination of deficiencies, in ICFR such that there is a **reasonable possibility that a material misstatement** of the registrant’s annual or interim financial statements **will not be prevented or detected** on a timely basis.
- Significant Deficiency²
 - a deficiency, or a combination of deficiencies, in internal control over financial reporting that is **less severe** than a material weakness, yet important enough to **merit attention by those responsible for oversight** of the registrant’s financial reporting.

¹ SEC 33-8809 - Amendments to Rules Regarding Management’s Report on Internal Control Over Financial Reporting

² SEC 33-8829 - Definition of the Term Significant Deficiency

Important Terms

- Materiality
 - Guidance in accounting and auditing literature is subjective, but essentially comes down to:
 - “what would be material to the reasonable investor when making an investment decision in the company’s securities.
 - Usually, this is 5 percent of the company’s pre-tax net income, but may be different when the company has losses or low profit levels; both quantitative and qualitative aspects must be considered.”

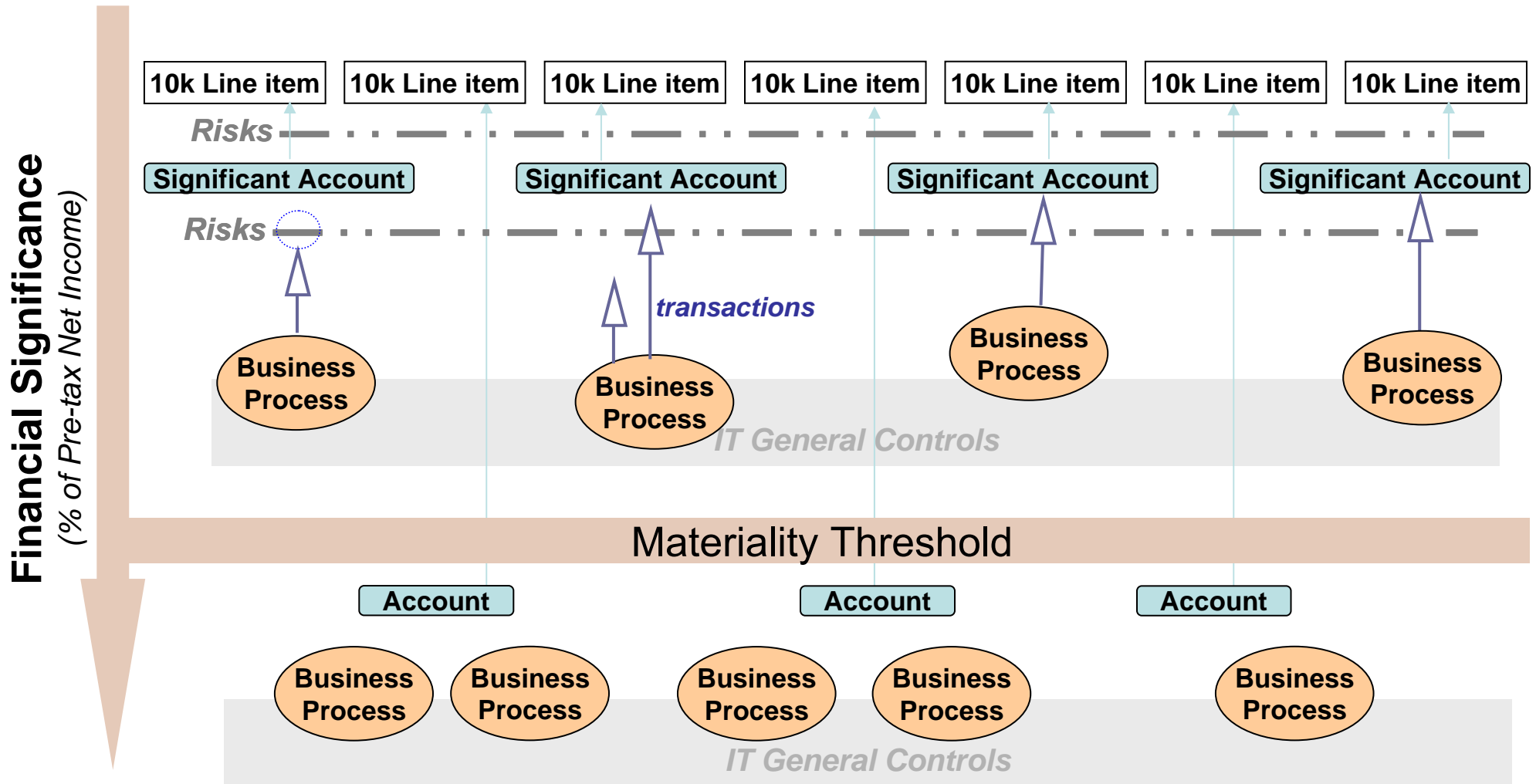


Important Terms

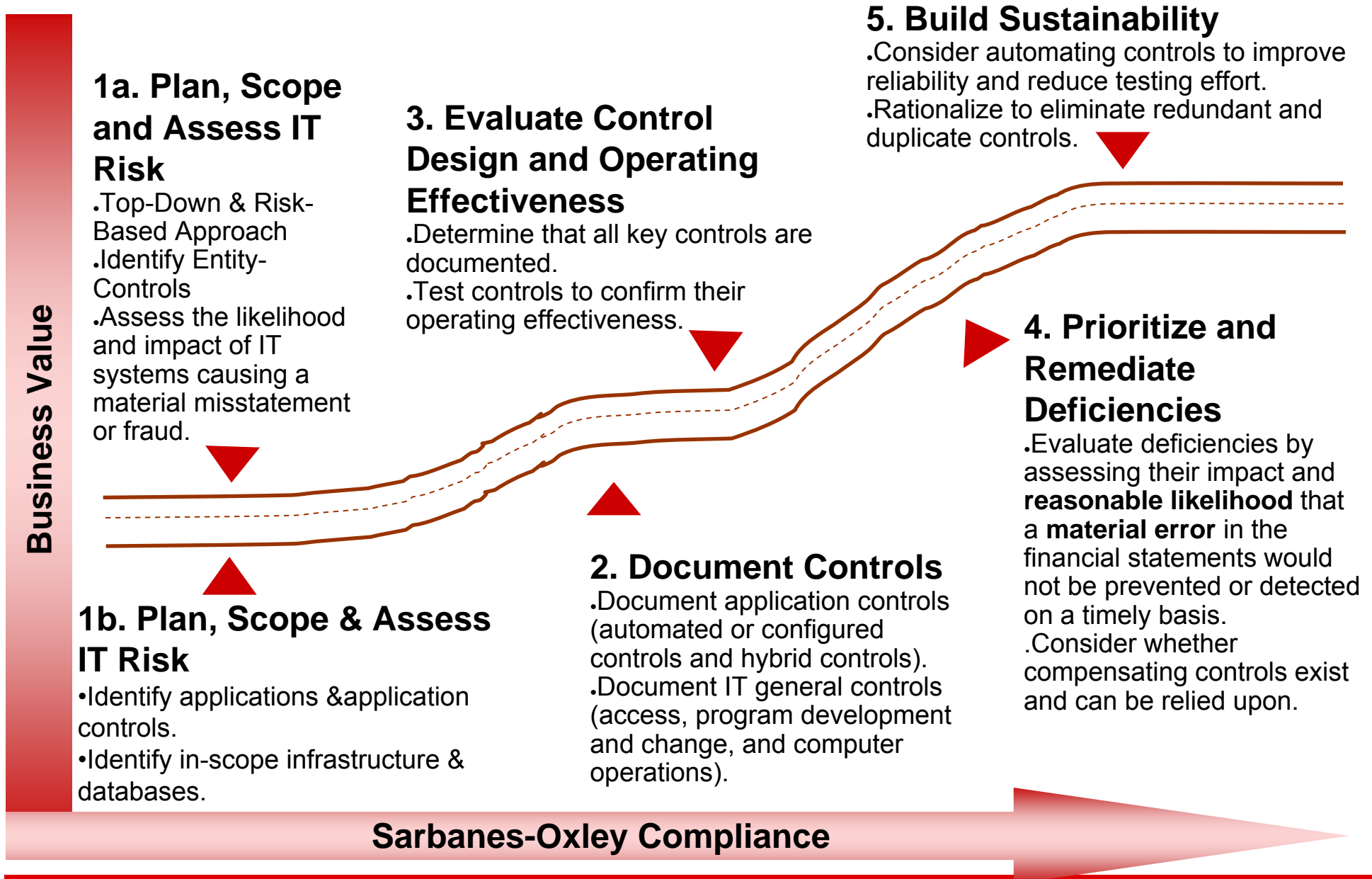
- Top-Down and Risk-Based Approach
 - Management should evaluate whether it has implemented controls that will achieve the objective of ICFR (that is, to provide reasonable assurance regarding the reliability of financial reporting).
 - The evaluation begins with the identification and assessment of the risks to reliable financial reporting (that is, materially accurate financial statements), including changes in those risks.
 - Management then evaluates whether it has controls placed in operation (that is, in use) that are designed to adequately address those risks.
 - Management ordinarily would consider the company's entity-level controls in both its assessment of risks and in identifying which controls adequately address the risks.”



Top-Down and Risk-Based Approach to Identifying Key Controls



IT SOX Compliance Road Map



Lessons Learned

Review of initial Section 404 IT compliance programs against the backdrop of SEC Interpretive Guidance and PCAOB AS5

Lessons Learned Observations

- Management has a great deal of flexibility in designing and implementing their Section 404 program — much more than is available to the external auditor.
- Many companies did not make changes to their SOX compliance programs after implementation nor use the SEC Management Guidance to their advantage.

Lessons Learned-Plan, Scope & Assess IT Risk

Lessons Learned	Actions to Consider
<p data-bbox="44 282 1024 537">Inadequate organization and reporting structures were established so IT could not be fully integrated into the overall Sarbanes-Oxley Steering Committee.</p> <p data-bbox="44 672 1031 992">Additionally, once programs were put in place, if the IT general controls (ITGCs) were not understood or considered, the process, tools, and metrics were adversely affected.</p>	<p data-bbox="1066 282 2039 532">Form an IT controls subcommittee that is integrated into & reports into an overall Sarbanes Oxley Steering Committee. Oversees:</p> <ul data-bbox="1178 558 2028 911" style="list-style-type: none"><li data-bbox="1178 558 1902 662">– IT Sarbanes-Oxley compliance process<li data-bbox="1178 683 2028 846">– facilitates communicate & integration into the overall Sarbanes-Oxley program<li data-bbox="1178 867 2003 911">– interfaces with the external auditors

Lessons Learned-Plan, Scope & Assess IT Risk

Lessons Learned	Actions to Consider
<p>SEC did not provide sufficient guidance related to the identification of the ITGCs.</p> <p>Some organizations having separated the identification of ITGCs manual and automated controls, with the finance function (or financial internal auditors) identifying the manual controls and the IT function (or IT auditors) identifying the automated controls.</p> <p>Responsibility for IT Controls was not properly defined.</p> <ul style="list-style-type: none"> -Identifying owners of business applications -Responsibility for application-level controls & significant spreadsheets <p>This approach is likely to lead to significant problems because it is not top-down, risk-based.</p>	<p>The identification of IT controls — both automated controls within business processes and IT general controls (ITGCs) — should be the result of a top-down and risk-based (TDRB) approach.</p> <p>Example: Understand & apply the GAIT Methodology from the Institute of Internal Auditors</p> <p>The team performing the identification should have a solid understanding of the financial statements, business processes and IT.</p> <p>The identification of risks & controls within IT should be integral to, and not separate from, management's TDRB approach to evaluating ICFR.</p>



Lessons Learned-Plan, Scope & Assess IT Risk

Lessons Learned	Actions to Consider
<p>Some companies adopted a methodology for Section 404 that was rules-based, leading to ineffective and inefficient assessments.</p> <p><i>Examples of rules-based activities:</i></p> <ul style="list-style-type: none"> • Testing every control in every situation. • Checklist approach to controls testing. • Determining that more than “x”-number of control deficiencies, without regard to significance, will always indicate material weakness. • Determining that specific deficiencies (e.g., failing to monitor the activities of the database administrator, or failing to have a comprehensive fraud assessment program) are always at least significant and probably material deficiencies. 	<p>Management should use judgment to develop & operate a continuing Section 404 program that is principles-based.</p> <p><i>Benefits of principles-based activities:</i></p> <p>The SEC Management Guidance and PCAOB AS5 are fundamentally principles-based approaches that emphasize the use of judgment by both management and the external auditor.</p> <p>Principles-based guidance provides significant flexibility in the TDRB approach. There are two major steps:</p> <ol style="list-style-type: none"> 1) Determining the scope of controls to include in testing; and 2) Determining the nature, timing and extent of testing procedures to perform.



Lessons Learned-Plan, Scope & Assess IT Risk

Lessons Learned	Actions to Consider
<p data-bbox="86 375 1035 591">The identification of key controls within ITGC can be complex, especially the first time it is done. It's easy to select too many controls to test.</p> <p data-bbox="86 721 1024 878">Controls that were assessed and tested that are not critical, resulted in unnecessary cost and diversion of resources</p> <p data-bbox="86 951 1026 1109">Controls that were key weren't tested, or were tested late in the process, presenting a risk to the assessment or audit</p>	<p data-bbox="1150 342 1997 732">Perform a "reasonable person" review. Take the opportunity to "step back" and review the ITGC selection to determine whether a reasonable person, also known as a prudent official, would consider the selection of key controls to be appropriate.</p>



Lessons Learned-Plan, Scope & IT Assess Risk

Lessons Learned	Actions to Consider
<p>Process documentation often became the testing objective instead of serving as an aid to identifying relevant control</p>	<p>Stop testing the process documentation controls.</p> <p>Documentation of a control policy or procedure provides no evidence to support the operating effectiveness of the control.</p>

Lessons Learned-Plan, Scope & Assess IT Risk

Lessons Learned	Actions to Consider
<p>Applications that were not “significant” were not taken out of scope and some applications that should have been included were not included until an issue was raised by the external auditor</p>	<p>“Significant applications” are those where there is critical IT functionality. While there may be risk to business operations if ITGCs relating to other applications fail, because these other applications do not have any critical IT functionality, ITGC failures would not result in a material error in the financial statements.</p> <p>Have your external auditor review & provide feedback on scope</p>

Lessons Learned-Evaluate Design & Operating Effectiveness (Testing)

Lessons Learned	Actions to Consider
<p>Testing deviations were automatically treated and reported as defects with zero deviations allowed or considered in confirming that the control is operating effectively</p>	<p>AS5 #48 states “Because effective internal control over financial reporting cannot, and does not, provide absolute assurance of achieving the company's control objectives, <u>an individual control does not necessarily have to operate without any deviation to be considered effective.</u>”</p> <p>Question: How many deviations in the performance of the control would be acceptable to still conclude that the control is operating effectively?</p>

Lessons Learned - Learned-Evaluate Design & Operating Effectiveness

Lessons Learned	Actions to Consider
<p>Business process-level / activity-level testing did not determine if an ITGC deficiency was the cause.</p>	<p>For deficiencies identified resulting from application-level control point testing at the business process / activity level, ITGC impact should be analyzed.</p> <p>If the application level defect resulted from an ITGC deficiency, an ITGC deficiency should be recorded.</p>

Lessons Learned - Learned-Evaluate Design & Operating Effectiveness

Lessons Learned	Actions to Consider
<p>Impact to application controls was not considered when ITGC defects were identified</p> <p>Without this being done there is no way to determine the risk and impact resulting from the testing exceptions</p>	<p>Ensure the impact to the application level controls is considered</p> <p><i>PCAOB – Although IT general control deficiencies do not result in financial statement misstatements directly, an associated ineffective application control may lead to misstatements. Therefore, the significance of an IT general control deficiency should be evaluated in relation to its effect on application controls, that is, whether the associated application controls are ineffective.</i></p>



Lessons Learned

Prioritize & Remediate Deficiencies

Lessons Learned	Actions to Consider
<p>In some cases, rather than identifying relevant controls & deficiencies, the external auditor challenged management's assessment.</p> <p>Management accepted the external auditor's assessment and performed additional work</p> <p>This led to some control deficiencies being identified late in the year not allowing for sufficient time for remediation.</p>	<p>Communicate ongoing with your external auditor to help ensure that the relevant controls identified meet the external auditor's scope and expectation</p> <p>This will help avoid the need to perform additional work late in the year.</p>



Lessons Learned

Build Sustainability

Lessons Learned	Actions to Consider
<p>Companies did not look for ways to improve the process / program</p> <p>Once a year is completed, the program for the next year is started</p> <p>If an annual assessment was completed, not all key stakeholders participated leading to missed opportunities that could result in time & cost savings to the compliance process</p>	<p>Hold post implementation / annual assessment with all stakeholders to determine how the Sarbanes-Oxley process can be improved</p> <p>Management can identify lessons learned & implement cost-effective plans for the following year</p> <p>Establish a position and make it their responsibility to perform an annual IT SOX program evaluation leveraging current SEC & PCAOB Management Guidance. Develop a program assessment guide to assist in the annual evaluation</p>



SOX 404 Study / Web Survey *

Table 17 - Impact of 2007 reforms on cost of compliance for Section 404(b) companies

		N	decrease/none/increase		
			-1	0	1
Impact of Management Guidance on total cost of compliance	< 75M (1)	40	47.5%	50.0%	2.5%
	75-700M (2)	376	30.3%	65.7%	4.0%
	>700M (3)	364	45.3%	53.3%	1.4%
Impact of Auditing Standard No. 5 on total cost of compliance	< 75M (1)	41	48.8%	46.3%	4.9%
	75-700M (2)	382	47.9%	46.9%	5.2%
	>700M (3)	373	66.5%	31.4%	2.1%
Combined impact of Management Guidance and AS5 on total compliance cost	< 75M (1)	40	55.0%	40.0%	5.0%
	75-700M (2)	382	48.2%	46.9%	5.0%
	>700M (3)	357	69.2%	29.4%	1.4%

The evidence from the survey response data shows that the cost of Section 404 compliance decreased following the Commission's reforms introduced in 2007

*Office of Economic Analysis, U.S. Securities and Exchange Commission, September 2009. **Study of the Sarbanes-Oxley Act of 2002 Section 404 Internal Control over Financial Reporting Requirements.**
http://www.sec.gov/news/studies/2009/sox-404_study.pdf:



Summary

- Between 2004 and 2007 changes were made to the SEC Management Guidance and PCAOB AS5 to address industry concerns and feedback.
- Some companies embraced the guidance & responded by making changes to their SOX and IT SOX programs that in some cases reduced the cost of compliance
- We encourage you to validate how your company has responded to the changes and determine if an opportunity exists to make changes that not only reduce compliance cost but provides an approach that achieves the “spirit of SOX”.
- Through this journey, ongoing & interlocked approach & communication with External Auditor is a critical to successful change & meeting requirements



Key References / Resources

Michael J. Ramos, 2006. *How to Comply with Sarbanes-Oxley Section 404: Assessing the Effectiveness of Internal Control*, 2nd edition. Wiley.

Christopher Fox, Paul Zonneveld and IT Governance Institute, September 2006. *IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting*, 2nd Edition.

The Institute of Internal Auditors, January 2008. *Sarbanes-Oxley Section 404: A Guide for Management by Internal Controls Practitioners*, 2nd edition. <http://www.theiia.org/download.cfm?file=31866>

Securities and Exchange Commission, June 20, 2007. Release No. 33-8810, *Commission Guidance Regarding Management's Report on Internal Control Over Financial Reporting Under Section 13(a) or 15(d) of the Securities Exchange Act of 1934*. Effective Date: June 27, 2007. <http://www.sec.gov/rules/interp/2007/33-8810.pdf>

Securities and Exchange Commission, June 20, 2007. Release No. 33-8809, *Amendments to Rules Regarding Management's Report on Internal Control Over Financial Reporting*. Effective Date: August 27, 2007. <http://www.sec.gov/rules/final/2007/33-8809.pdf>

Securities and Exchange Commission, August 3, 2007. Release No. 33-8829, *Definition of the Term Significant Deficiency*. Effective Date: September 10, 2007. <http://www.sec.gov/rules/final/2007/33-8829.pdf>

PCAOB, July 25, 2007. Release No. 2007-005A, *Auditing Standard No. 5 - An Audit of Internal Control Over Financial Reporting That Is Integrated with An Audit of Financial Statements*. Effective Date: Fiscal years ending on or after November 15, 2007. http://pcaobus.org/Standards/Auditing/Pages/Auditing_Standard_5.aspx

PCAOB, June 18, 2004. Release No. 2004-001, *Auditing Standard No. 2 - An Audit of Internal Control Over Financial Reporting Performed in Conjunction With an Audit of Financial Statements*. Effective Date: Fiscal years ending on or after November 15, 2004. http://pcaobus.org/Standards/Auditing/Pages/Auditing_Standard_2.aspx



More Sarbanes-Oxley Resources

From:

U.S. Securities and Exchange Commission
The Laws That Govern the Securities Industry

<http://www.sec.gov/about/laws.shtml>

Sarbanes-Oxley Act of 2002

On July 30, 2002, President Bush signed into law the Sarbanes-Oxley Act of 2002, which he characterized as "the most far reaching reforms of American business practices since the time of Franklin Delano Roosevelt." The Act mandated a number of reforms to enhance corporate responsibility, enhance financial disclosures and combat corporate and accounting fraud, and created the "Public Company Accounting Oversight Board," also known as the PCAOB, to oversee the activities of the auditing profession. The full text of the Act is available at: <http://uscode.house.gov/download/pls/15C98.txt>. (Please check the [Classification Tables](#) maintained by the [US House of Representatives Office of the Law Revision Counsel](#) for updates to any of the laws.) You can find links to all Commission rulemaking and reports issued under the Sarbanes-Oxley Act at: <http://www.sec.gov/spotlight/sarbanes-oxley.htm>.



Questions?

Contact Information:

Sheila Gallimore – sgallimore@live.com

Roxanne Halverson – rhalverson@us.ibm.com



FIN

Thank you for your kind attention

