To hear Presenter please turn on computer speakers

If you cannot hear the presenter with your speakers you may call
213-286-1201 **Access Code: 483-379-784**
Webinar ID:316-784-337

SOX IT for Non Accelerated Filers

Using COSO Guidance for Smaller Public Companies

Lord & Benoit
Shining Light on Section 404 Compliance

Disclaimer

The literature contained herein is not intended to substitute authoritative literature published by the respective regulatory agencies. Professionals are advised to consult with legal and accounting authorities on all matters before implementing professional standards.

To hear Presenter please turn on computer speakers

If you cannot hear the presenter with your speakers you may call
213-286-1201 Access Code: 483-379-784
Webinar ID:316-784-337

Continuing Professional Education

- There will be instructions at the end of this seminar on obtaining CPE credit* for this webinar.
- To qualify you must attend at least 50 minutes of this webinar.

* *Please note: State Boards of Accountancy have final authority on the acceptance of individual courses for CPE credit.*

Lord & Benoit is not registered with NASBA.

Continuing Professional Education (cont.)

Please turn on computer speakers to hear presenter

Copies of Slides will be available on website:

www.Section404.org

Education, Training & Seminars

Update on SOX 404

- SEC

- PCOAB

PCAOB®

- COSO

SOX Guidance

- Internal Control over Financial Reporting — Guidance for Smaller Public Companies
- Guidance on Monitoring Internal Control Systems

www.coso.org

Internal Control Components

Top Down Risk-Based

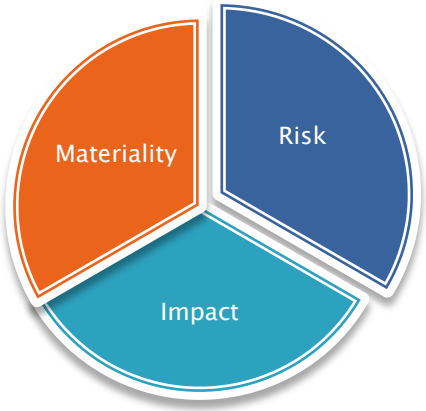
Financial Statement

Significant Accounts

IT Assets

Control Objectives

Key Controls



Risk-Based Definition

- Risk-based means:

- *Focusing on quantitative and qualitative factors that potentially affect the reliability of financial reporting*

and

- *Identifying where in transaction processing or other activities related to financial statement preparation something could go wrong.*

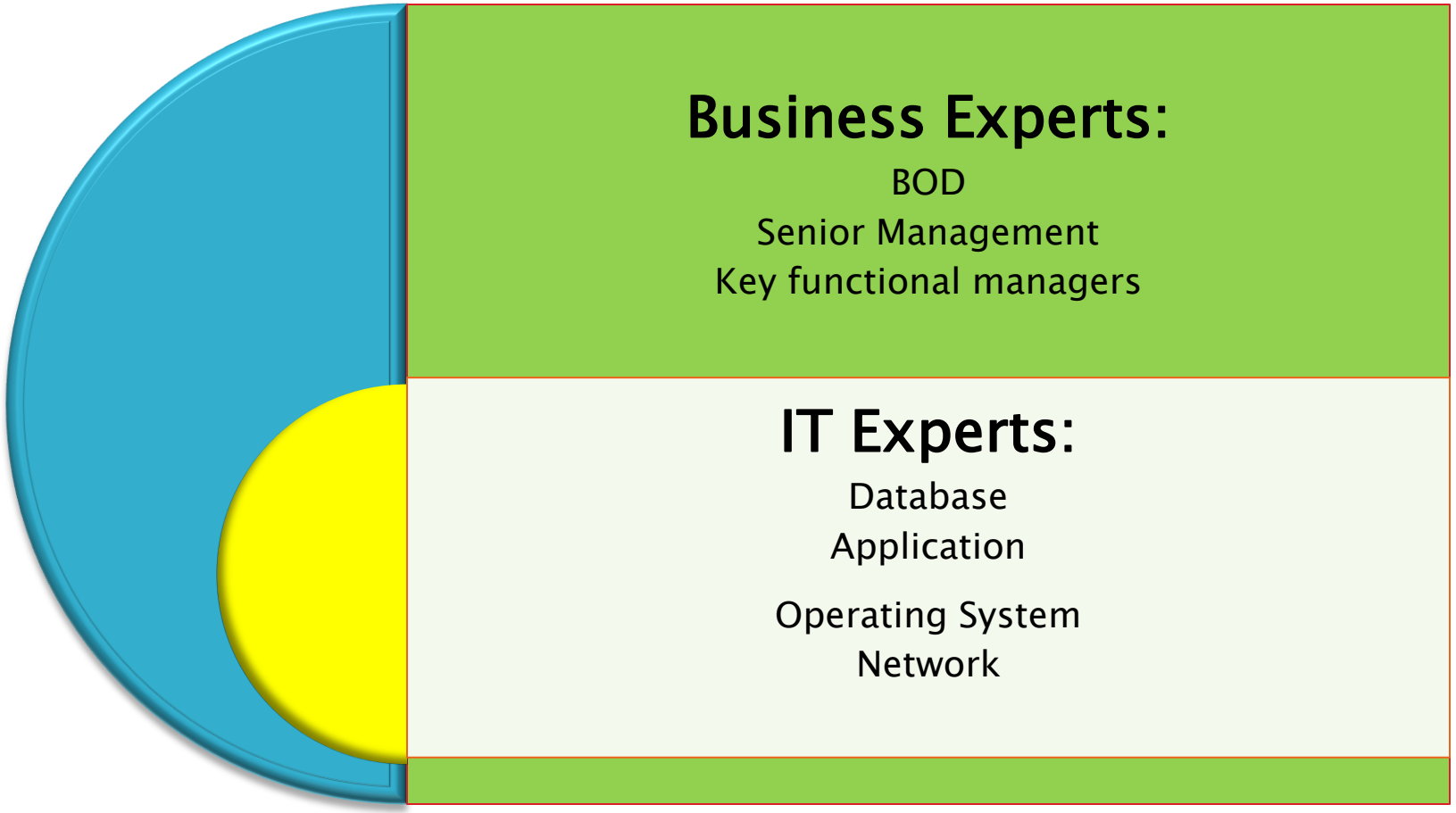
The "Wrong" Controls?

- Controls that are key may not be tested, or may be tested late in the process, presenting a peril to *the results* of the assessment or audit.
- Controls may be assessed and tested that are not critical, resulting in *unnecessary cost* and diversion of resources.

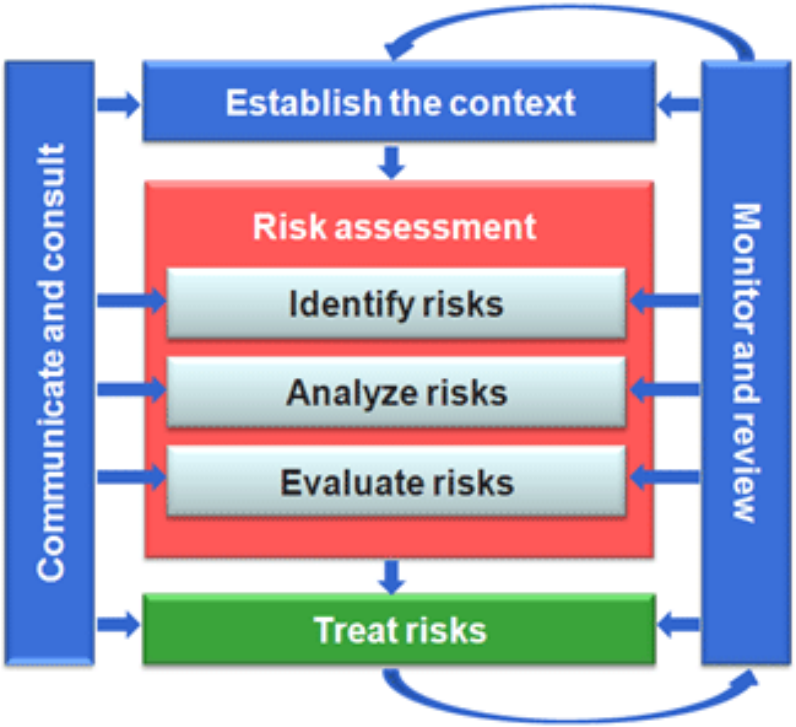
IT Risk Methodology

- Identify and focus on critical information assets (staff, systems and processes)
- Consider the relationships among critical assets
- Evaluate risks in operational context
- Establish control objectives & key controls to reduce risks to an acceptable level

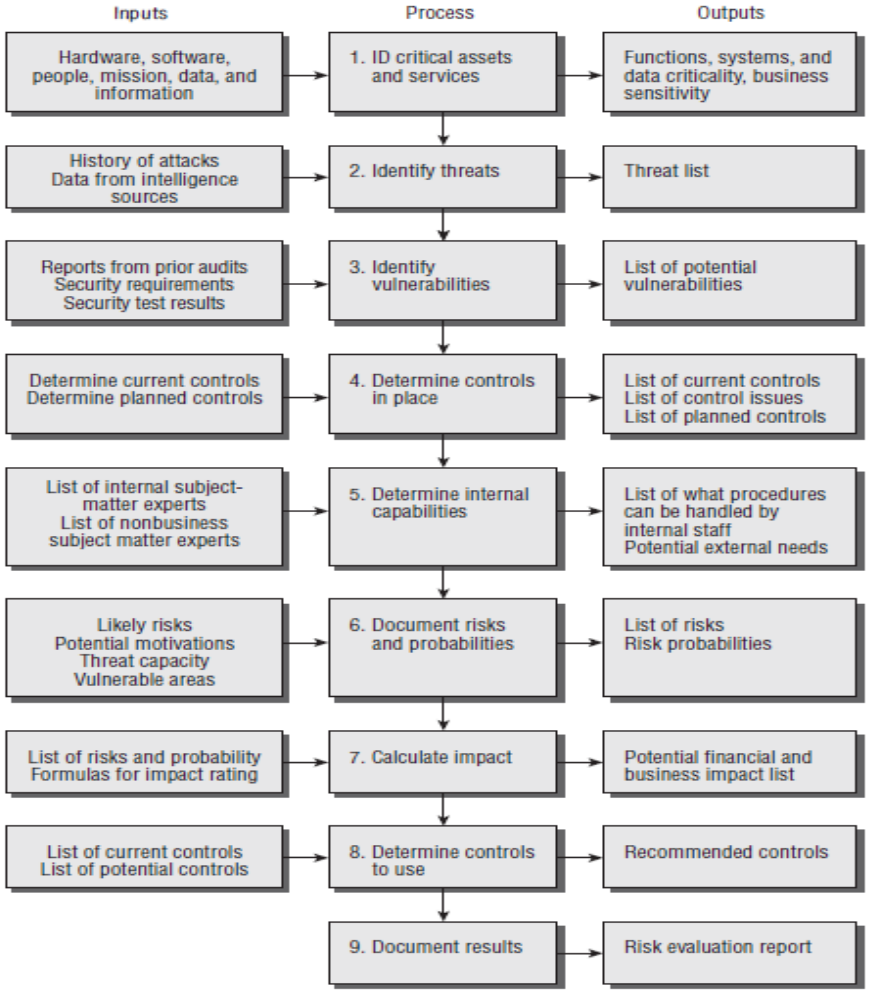
Who Should Identify ITGC Risks?



Risk Assessment



Risk Analysis Flowchart



Information Technology Area	Risk	General Computer Control	Preventive / Detective	Manual / Automated
Change Management	Incorrect changes are made to systems, applications, infrastructure and databases, adversely affecting the reliability of financial reporting.			
Security and Access – Logical	Improper use, disclosure, modification, or loss of critical financial data adversely affecting the reliability of financial reporting.	Password expiration Authorized user accounts Recertification of access		
Security and Access – Physical This section refers to data centers. In some smaller companies, network servers and communication equipment may comprise the entirety of the data center.	Improper use, disclosure, modification, or loss of critical financial data adversely affecting the reliability of financial reporting.			
Computer Operations – Data Backup	Lost or corrupted critical financial data is not recoverable, adversely affecting the reliability of financial reporting.			
Computer Operations – Third-Party Vendor Management	Inappropriate operations by a third party adversely affect data captured, processes, or reported to the company.			
Application Controls	Procedures in application programs to help ensure completeness and accuracy of transaction processing are ineffectively designed or not operating as intended.			

Mapping Business Sub-Processes to IT

Business Process and Sub-Process	Overall Rating	Application Name	Database	Operating System	Critical Spreadsheet Name	Supported by a Third Party	Hosted by a Third Party Provider
Cash Management	**H**	MS Dynamics	MS SQL	Windows 2008	N/A	Yes	Yes
Investment Securities							
Order Processing							
Credit and Collections							
Revenue Recognition							
Purchasing to Payables							
A/P and Cash Disbursements							
Employee Master File Maintenance							
Process Payroll							

IT Company Level Controls

1. **Integrity and Ethical Values** – Sound integrity and ethical values, particularly of top management, are developed and understood and set the standard of conduct for financial reporting. [Carry over to IT—Acceptable Use Policy?]

2. **Board of Directors** – The board of directors understands and exercises oversight responsibility related to financial reporting and related internal control. [IT Governance; IT Steering Committee]

3. **Management's Philosophy and Operating Style** – Management's philosophy and operating style support achieving effective internal control over financial reporting.

4. **Organizational Structure** – The company's organizational structure supports effective internal control over financial reporting.

5. **Financial Reporting Competencies** – The company retains individuals competent in financial reporting and related oversight roles. [IT Competency]

6. **Authority and Responsibility** – Management and employees are assigned appropriate levels of authority and responsibility to facilitate effective internal control over financial reporting. [Is IT Segregation of Duties considered?]

7. **Human Resources** – Human resource policies and practices are designed. [IT Policies and Procedures]

Design of Control Testing

- After establishing key IT controls, a “design test should be performed.
- Primarily accomplished through inquiry, observation and “walk-through’s”

Operational Testing

- Establish a Control and Test matrix that:
- Identifies Control Objective, Risks and key control that mitigate identified risks
- Establish valid test including sample size to determine if control is operating correctly.
- Document deficiencies; develop remediation plans

Summary of Deficiencies

- A summary of deficiencies should be compiled that outlines the deficiency found, its severity and a remediation plan to address.

  Remediation solutions can/should be re-tested to ensure proper operation prior to year-end.

Key IT Findings

- Sarbanes-Oxley Section 404: 10 Threats to Compliance for Smaller Companies—
  "A Primer for Companies that need to comply with SOX 404(b) for FY ending in December 2009"

www.section404.org

Other Tips

- Risk Assessment and Company level controls
- Right-sized documentation
- Objectivity & competence
- Third-party IT support
- Relevant remediation solutions
- Focus on monitoring activities

Monitoring: Nature & Purpose

- The performance of ongoing and/or separate evaluations that are critical in determining whether internal controls function over time.

- To identify internal control deficiencies and communicate them in a timely manner to those parties responsible for taking corrective action and to management and the board as appropriate.

Contact Us

800.404.7794 x207

mikem@section404.com

www.section404.org

Continuing Professional Education

If you would like CPE credit* for this webinar:

1. Please e-mail LizK@Lordandbenoit.com today.
2. Be sure to include your full name in the e-mail
3. You will be asked to complete an Evaluation Form and a Survey Questionnaire

Requests for CPE credit must be received by the end of class today

We will send you:

1. Certificate of Completion form
2. Copies of Slides are available on website www.section404.org

Please note: State Boards of Accountancy have final authority on the acceptance of individual courses for CPE credit.

**As mentioned earlier, Lord & Benoit is not registered with NASBA*

Lord & Benoit
Shining Light on Section 404 Compliance