Is Your IT Audit Strategy Properly Focused?

Houston Chapter – ISACA

November 19, 2009

IT Audit Considerations

- **Is your IT audit strategy addressing the most relevant business objectives and IT risks to your organization?**
- **Is your IT audit strategy in line with best practices?**
- **Are you providing noticeable value to your stakeholders?**

Risk and Strategy Assessment Considerations

- **Value campaign (enhancing vs. maintaining)**
- **Business objectives**
- **Stakeholders' views**
- **IT environment (complexity)**
- **Risks**
  - **Control frameworks (CoBiT, PCI, etc.)**
- **Functional audit strategies**
- **Emerging & hot topics**

Organizational Risks

- **Financial**
- **Operational**
- **Strategic**
- **Compliance**
- **System**

System Risks

- **IT governance**
  - **IT policies & procedures**
  - **Executive oversight**
  - **IT strategic planning**
  - **Knowledgeable IT support resources**
- **IT compliance**
  - **Internal compliance to business objectives and IT policies and procedures**
  - **External compliance to regulations affecting technology**

System Risks (continued)

- **IT asset management**
  - **Comprehensive IT inventory listing**
  - **Routine inspection and maintenance**
- **Data quality and retention**
  - **Validity, accuracy and completeness of data (data conversions, interfaces, data processing)**
  - **Data standardizations**
  - **Backup and storage**
  - **Adherence to data retention guidance**

System Risks (continued)

- **Data security and privacy**
  - **Unauthorized access and use restrictions**
  - **Data disclosure restrictions**
  - **Access monitoring**
- **IT development and maintenance**
  - **Development procedures**
  - **Project management**
  - **Maintenance procedures**
  - **Separate environments with restricted access**

System Risks (continued)

- **IT business systems (ERPs)**
  - **Out-of-date, unsupported**
  - **Alignment with business objectives**
  - **Scalability (design and use)**
- **Disruption prevention and recovery**
  - **Physical security**
  - **Environmental protection**
  - **Virus protection**
  - **Intrusion prevention and detection**

System Risks (continued)

- **Disruption prevention and recovery (continued)**
  - **Disaster recovery**
  - **Business continuity**
- **IT Outsourcing**
  - **Physical security**
  - **Data retention**
  - **Availability**
  - **Governance**
  - **Compliance**

Common Risk Assessment Tools

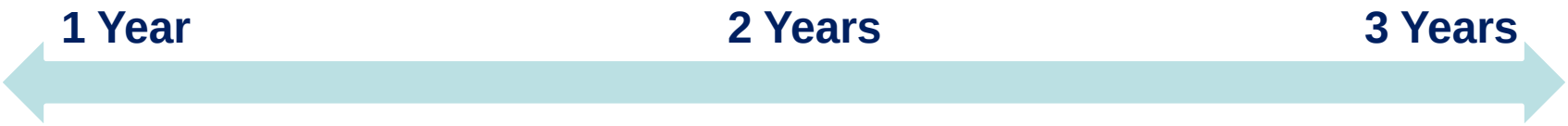
- **Excel / Access**
- **Paisley Enterprise GRC**
- **Resolver Risk**
- **MetricStream**
- **TeamRisk (part of TeamMate)**
- **RiskWatch**
- **www.auditsoftware.net/risk_management_software.html**

Weighing Risk

- **Factors for weighing risk**
  - **Qualitative risks**
    - **Significant importance to the organization**
    - **Difficult to quantify (monetize)**
  - **Quantitative risks**
    - **Loss of assets**
    - **Loss of earnings**
    - **Expenses and penalties**
  - **Impact**
  - **Likelihood**

Update Frequency

- **IT Risk assessment (every 1 to 3 years)**
- **IT Audit plan (every 1 to 3 years)**



Significant Change

- Business objectives
- Mergers & Acquisitions
- ERP change / process change
- Regulatory requirements

Moderate Change

- Expansion of existing systems
- System change / no process change

Minimal Change

Update Frequency (continued)

- **Periodic assessment updates**
  - **Stakeholder views**
  - **Change**
    - **Business objectives**
    - **Business operations**
      - **Mergers and acquisitions**
    - **System change**
    - **New and increased existing threats to security**
    - **Emerging topics**
      - **New legislation**
      - **New standards**

Best Practice Considerations

- **Do each of your IT Internal Auditors know your organization's business objectives?**
- **Do you know all of the technologies used by your organization and the purpose for each and is this documented?**
- **Is your IT risk assessment / IT audit strategy utilizing a formal framework (like CoBiT)?**

Best Practice Considerations (continued)

- **Do you emphasize the need for formal policies and procedures throughout the IT function?**
- **Is your IT audit function integrated with your functional audit?**
  - **Are IT audits on applications coupled with functional audits affected by those applications?**
  - **Do your IT auditors aid in functional audits?**

Best Practice Considerations (continued)

- **Do you have the right resources (expertise) performing each audit?**
  - **Relevant ERP specialists on ERP audits**
  - **Attack and penetration specialists on intrusion audits**
  - **Knowledgeable staff using CAATs software**

Best Practice Considerations (continued)

- **Do you maximize automation within your audits?**
  - **Do you know where relevant data is stored within existing databases and are you requesting source data vs. reports?**
  - **Are you utilizing automated auditing tools (with built in evaluation functions) when evaluating extracted data?**
  - **Do you leverage off of past audit scripts to create efficiencies in your present audits?**

Emerging & Hot Topics

- **Emerging topics**
  - **XBRL reporting**
    - **Phased in compliance – company size**
    - **No third party assurance**
  - **Climate control reporting**
    - **Reliability of measurement systems**
    - **EPA reporting mandates**
  - **Cloud computing (Gartner article)**
    - **Privileged user access**
    - **Regulatory compliance**

Emerging & Hot Topics (continued)

- **Emerging topics (continued)**
  - **Cloud Computing (continued)**
    - **Data location**
    - **Data segregation**
    - **Recovery**
    - **Investigative support**
  - **IT Outsourcing**
    - **Increased data access**
    - **Regulatory compliance**
    - **Dependency on third party**
    - **Legal challenges**

Emerging & Hot Topics (continued)

- **Hot topics**
  - **PCI compliance**
    - **Compliance driven by payment card company**
    - **Most deadlines already past**
  - **HIPAA compliance**
    - **ARRA 2009 – tiered civil penalties**
    - **Criminal penalties based on exposure**
  - **Contract compliance**
  - **License fee compliance**

Measuring Value

- **Monetary savings**
  - **Dollars saved**
- **Efficiency gains**
  - **Doing more with equal or less resources**
- **Process improvement**
  - **Increased effectiveness**
  - **Better quality**
  - **Better safety**

Strategic Items Producing Measurable Value

- **Maximize your external auditor's reliance on your controls testing**
  - **Internal fees less than external fees**
- **Controls Optimization**
  - **Minimize the quantity of controls for Sox audits**
    - **You may be spending time in areas you have no intention on addressing in your IT audit plan**
  - **Maximize automated controls (preventative vs. detective)**

Strategic Items Producing Measurable Value (cont.)

- **Real-time assessment and recommendations during implementations**
  - **Reporting depends on purpose and audience**
  - **Post implementation corrections are several times more expensive to correct**
    - **Reinvest in training**
    - **Business intrusion**
    - **Tie up IT support**

Strategic Items Producing Measurable Value (cont.)

- **Recommend maximizing the use of existing systems and automated controls**
  - **Maximize ERP functionality; minimize the use of smaller unnecessary systems**
  - **Computer automation is cheaper than manual efforts**
- **Proactively address emerging topics; bring recommendations to the table**
  - **Early assessments and recommendations may help management in decision making**

Strategic Items Producing Measurable Value (cont.)

- **Integrate with Internal Audit and maximize automation in testing**
  - **Maximize the efficiency of each audit performed and limit organization intrusion**

Conclusion

- **Do not silo your IT audits (i.e., consider them independent of the business); IT affects most (if not all) organization processes in some manner**
- **No one IT audit approach is best for every organization (customize as needed)**
- **Consider the cost/benefit when creating IT audit strategies and performing individual IT audits**

Questions?