
CONFESSIONS OF AN IT AUDITOR

PHOCUS 2003

Joel Lanz, CPA, CISA, CISSP.

www.itriskmgt.com

jlantz@itriskmgt.com

Agenda

- Background on auditing and auditors
 - what they do
 - how to prepare
 - minimizing bad reports
 - Interactive discussion on dealing with audits and audit issues
-

Joel's Audit Experience

- Over 22 years of IT risk management experience ranging from one-person “IT shops” to global organizations – specializing in privacy-related industries (e.g., banking and insurance)
 - Principal of a niche technology risk management CPA practice, with prior experience as a Big 5 Technology Risk Partner and an Internal Audit Vice President
 - Adjunct Professor at the School of Professional Accountancy, College of Management, C.W. Post Campus of Long Island University.
 - Member, NYSSCPA Technology Assurance Committee
 - Professional Certifications in addition to CPA
 - Certified Information Systems Security Professional (CISSP)
 - Certified Information Systems Auditor (CISA)
 - Certified Fraud Examiner (CFE)
 - AICPA's Certified Information Technology Professional (CITP)
 - Publications, etc., etc.
-

What does the auditor accomplish in a typical audit?

- Ensures accuracy of records.
 - Provides cost analysis of historical trends.
 - Evaluates internal controls.
 - Supports the external auditors.
 - Performs due diligence of pending subsidiary purchases.
 - Documents and analyzes processes and costs.
 - Analyzes task performance in functional areas.
 - Surveys customers to determine satisfaction.
 - Evaluates costs and benefits.
-

What else does the auditor accomplish?

- Benchmarks performance and best practices.
 - Confirms internal and external compliance with laws, regulations, policies, and procedures.
 - Ensures compliance with contract terms and conditions.
 - Compares records with physical assets.
 - Reconciles independent and corporate records.
 - Reviews new system development projects.
 - Evaluates computer and software application controls.
 - Investigates alleged fraud situations.
-

The Evolving Role of the IT Auditor

- Traditional Role
 - After the fact
 - Subservient to the financial/operational auditor
 - Emphasis on IT department controls
 - Evolving Role
 - SAS 94 enhances impact of IT on the financial audit
 - For other auditors – get the lay of land – where should we focus our audit resources
 - Computer assisted audit techniques
 - Application strengths and exposures
 - For business managers – a helping hand
 - Pre-implementation – make changes before implementation
 - Security – guidance on increasingly complex area
 - Overall IT Governance
-

IT Governance Defined by Robert S. Roussey, ISACA President

“A focus on the leadership, organizational structures and processes to ensure that IT sustains and extends an entity’s strategies and objectives in the creation and preservation of values and wealth”

Roussey's Perspective on Manager and Audit Involvement with IT Governance

IMPACT ON MANAGERS

- ❑ Align IT strategy with business goals
- ❑ Cascade strategy and goals down into the organization
- ❑ Set up organizational structures that facilitate strategy implementation
- ❑ Adopt an IT control and governance framework
- ❑ Provide IT infrastructures that facilitate creation and sharing of business information
- ❑ Embed responsibilities for risk management in the organization
- ❑ Focus on important IT processes and core IT competencies
- ❑ Measure performance (Balanced Business Scorecard)

IMPACT ON AUDITORS

- ❑ Obtain an understanding about IT Governance
 - ❑ Get the Board and Management to focus on the issues in the previous two slides
 - ❑ Recommend the adoption of an IT control and governance framework, such as COBIT
 - ❑ Set up organizational structures in your areas that facilitate a strategic implementation of such a framework
 - ❑ Measure your own performance (Balanced Business Scorecard)
-

But it's only IT and controls over IT— do we really need to do this?

- Enterprise may not be able to exist without IT
 - Enterprise is highly dependent on business models predicated on IT
 - Inability to support revenue streams without automation
 - Inability to comply with regulations or contractual service levels without IT
 - IT involves substantial investments
 - Actual value of information is understated
-

Types of Audits

- External or Financial
 - Internal or Operational
 - Examiner
 - Functional Specialist
 - Business Function
 - Trust
 - Compliance
 - Credit Risk and Quality
 - Financial Risk (e.g., Derivatives, asset/liability)
 - Information Technology
-

External or Financial Audit

- Primary purpose in to express an opinion, using GAAS (auditing standards) on the financial statements prepared using GAAP (accounting principles).
 - Requires CPA license to sign the opinion
 - Needs to also attest to FDICIA and SOX
 - Impact of recent corporate scandals
 - PCAOB vs. ASB
 - “administrative” documentation to comply with SOX
-

What is Internal Auditing?

- Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

Source: The Institute of Internal Auditors

Risk Management Expertise

- Internal Audit (IA) provides a broad range of audit services designed to help the organization meet its objectives. One of IA's key roles is to monitor risks and ensure that the controls in place are adequate to mitigate those risks.
 - Typically IA is a corporate governance cornerstone —along with the board, executive management, and the external auditors.
 - IA can help you comply with new legislation and regulations for enhanced corporate governance.
-

What should you expect from your internal audit?

- ❑ An objective assessment of your operations, and share ideas for best practices.
 - ❑ Counsel for improving controls, processes and procedures, performance, and risk management.
 - ❑ Suggested ways for reducing costs, enhancing revenues, and improving profits.
 - ❑ Competent consulting, assurance, and facilitation services.
-

Examiner

- Not as easy as you think
 - Regulatory burden vs. best practice
 - Best practice vs. acceptable practice
 - “Open-book” examination
 - “Examiner Risk”
-

What does this all mean for the Ops & Sys Executive?

Joel's Rules of Success in Dealing with Auditors (or Examiners)

- Manage the audit
 - Appreciate the influence of auditors within the enterprise
 - Know how the audit process works
 - Prepare for the audit by studying the exam questions
 - Learn the advantages of and partner with audit
-

Manage the Audit

- Understand the type of audit you are involved with
 - Find out about the auditor's backgrounds – what are their strengths, weaknesses and paradigms
 - Appoint a liaison to facilitate, coordinate and maximize everyone's productivity
 - What's the game plan (including estimated dates)
 - Identify misconceptions early and correct
 - To the extent possible, implement recommendations ASAP – even before the end of the audit
 - Minimize surprises
 - Provide information requested in a timely manner
-

Appreciate the Influence of Auditors

- One whisper is worth more than a thousand words
 - Acceptable vs. Good vs. Best Practices
 - Use standard like COBIT to help manage expectations
 - Early and respectable contact for outsiders
 - The “eyes and ears” of whom?
 - Identify vested interests (especially external auditors and regulators)
-

Know How the Audit Process Works

- ❑ Planning
 - ❑ Gaining and confirming understanding
 - ❑ Evaluate controls
 - ❑ Consider whether to continue and develop audit program
 - ❑ Execute audit program
 - ❑ Clear exceptions
 - ❑ Develop draft report
 - ❑ Issue final report
 - ❑ Follow-up on recommendations
-

Prepare for the Audit by Studying the Exam Questions

- Regulatory Exams
 - The new FFIEC IT Examination Handbook for Information Security
 - Tier 1 – Everything
 - Tier 2 – Depends
 - First of Others
 - 501(b) exam procedures
 - FDIC General Controls Workprogram (12/02)
 - OTS Vendor Management Program (could be hint of what's to come from the FFIEC)
 - Audit Programs
 - ISACA's COBIT (www.itgovernance.org)
 - ISACA's Knowledgebase (www.isaca.org)
 - Auditors sharing audit workprograms (www.auditnet.org)
 - Recognized professional references
 - Practical IT Auditing (Warren, Gorham and Lamont)
 - Auerbach EDP Auditing and Data Security Service References
-

Learn the Advantages and Partner with Audit

- Build “the right” controls into the process
 - Gain consensus on the right mix of risk vs. control
 - COBIT standard provides some benchmark for this
 - COBIT small business version due out in the summer – a standard for bankers to watch out for.
 - Leverage the technology risk assessment to get “buy-in” on prioritizing “control initiatives.”
-

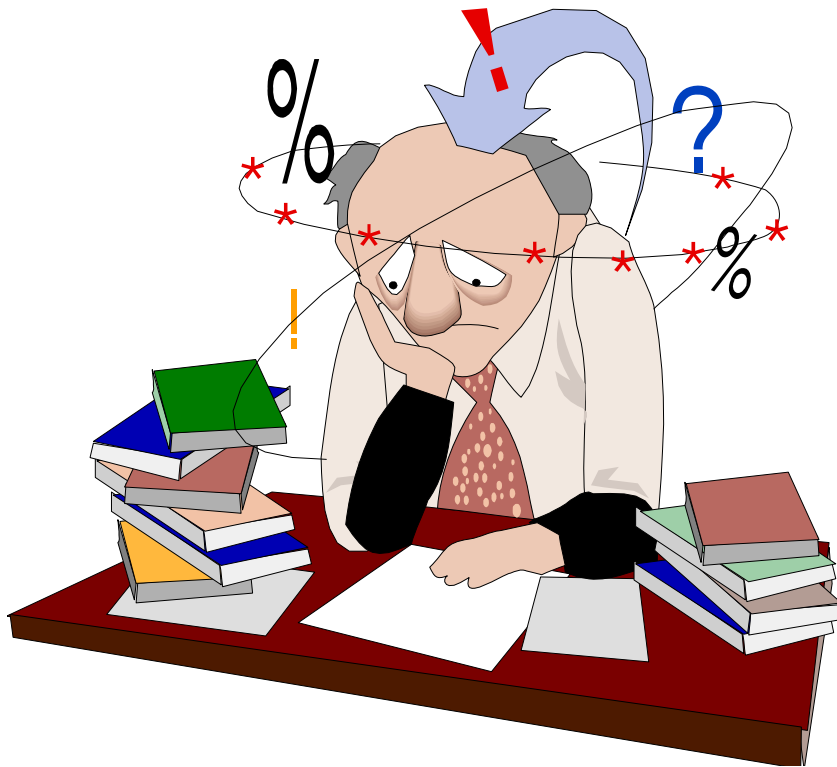
Anticipated IT Audit Issues in the Next 6-24 Months

- What will be the impact of SOX
 - How will IT Governance be addressed in the organization?
 - How do you perform a Technology Risk Assessment?
 - Are you doing vulnerability assessments on an ongoing basis?
 - What should an incident response plan contain?
 - How to prepare for computer forensics and fraud investigations?
 - How do you manage technology vendors and core application outsourcers?
 - How do you contract for security management services?
 - What is the role of insurance in managing technology risk?
 - How do you manage firewalls and public servers?
 - What are the challenges of effectively administering email and the PBX?
 - Are you in compliance with the new IT Examination Handbooks?
-

Your Questions on Dealing with Auditors

- How come?
 - Why do they?
 - How does?
 - What happens?
 - How do you?
 - When does?
 - Who decides?
-

QUESTIONS OR FURTHER INFO



Joel Lanz, Principal
Joel Lanz, CPA, P.C.
P.O. Box 597
Jericho, NY 117530597
PH: 516-933-3662
FX: 516-933-2885
jlanz@itriskmgt.com
www.joellanzcpa.com
www.itriskmgt.com
