



# A HITCHHIKER'S GUIDE TO IT GOVERNANCE AND RISK MANAGEMENT

---

Western Independent Bankers  
2004 Annual Cashiers/CFOs  
Conference & Expo



# Your Host

Joel Lanz, CPA/CITP, CISA, CISSP, CISM

---

- Vice Chairman, New York State Society of CPA's Technology Assurance Committee.
- Principal of a niche information technology risk management CPA practice, with prior experience as a Big 5 Business Risk Consulting and Assurance Partner and a Money Center Bank Internal Audit Vice President.
- Adjunct Professor at the School of Professional Accountancy, College of Management, C.W. Post Campus of Long Island University – Instruct required graduate course entitled "Advanced Assurance and Computer Auditing."
- Articles published in The Journal of Accountancy, CPA Journal, RMA Journal, Bank Accounting & Finance, Commercial Lending Review, AICPA InfoTech Update, IS Audit & Control Journal, Commercial Lending Review, etc.
- Contributed to four books and guides
- Over 23 years of IT risk management experience ranging from one-person "IT shops" to global organizations - focusing on depository and lending institutions.

---

JOEL LANZ, CPA, P.C

[www.bankingcpa.com](http://www.bankingcpa.com)



# Presentation Outline

---

- Introduction
- Presentation Assumptions
- Key Concepts
- Players
- While You've Been SOX'd – The FFIEC's Been Issuing
- Information Security
- IT Vendor Risk
- Good Banks Gone Bad
- Staying In Touch



# Presentation Assumptions

---

- Please ask questions throughout the presentation
- To maximize value to the audience, the following presentation assumptions were made:
  - To the extent possible, generally recognized and accepted standards and guidelines are leveraged. This strengthens support for identified IT risk management recommendations. It also provides better support for those implementing IT risk management programs in response to heightened regulatory expectations.
  - The audience already has a basic understanding of SOX and its implications on the IT environment, and is looking for additional information on IT governance and risk management practices in general – and IT regulatory compliance practices specifically.
  - ***WE'RE NOT TALKING BRAIN SURGERY HERE!!!*** Lots of good things are available on the internet – your challenge is to identify credible materials that you can leverage.
- The speaker will be available after the presentation (and during the conference) and welcomes any questions on the above or any topics discussed during the presentations

# In Case You Have an Urgent “Business” Matter to Attend to and Can’t Stay For the Entire Presentation



- “Managing information technology risk is the same as managing business risk. Only the words are different.”

*- Joel's client questioning Joel's fee*



# Anticipated IT Audit Issues in the Next 6-24 Months

---

- How will SOX change things especially proactive control monitoring?
- How will IT Governance be addressed in the organization?
- How well do you perform a Technology Risk Assessment?
- Are you doing vulnerability assessments on an ongoing basis?
- What should an incident response plan contain?
- 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 well do you or your vendor manage firewalls and public servers?
- Are you in compliance with the new IT Examination Handbooks?



# Key Players

---

- Regulatory (Banking) – ([www.ffiec.gov](http://www.ffiec.gov))
  - Technology-related issues, usually but not always, are the result of interagency efforts (e.g., FFIEC)
  - Already issued include Security, BCP, IT Audit, Fedline, Retail Payments, Technology Providers and eBanking
  - Additional planned books include outsourcing, management, development and acquisition, operations and wholesale payments.



# Key Players (cont.)

---

- PCAOB
  - PCAOB Auditing Standard No. 2
  - IT concerns focused on general controls
    - Program Development
    - Program Changes
    - Computer Operations
    - Access to Programs and Data
- AICPA ([www.aicpa.org](http://www.aicpa.org))
  - SAS 70, SAS 94
  - Trust Services



## Key Players (cont.)

---

- Information Systems Audit and Control Association (ISACA) ([www.isaca.org](http://www.isaca.org))
  - Professional association of IT Auditors
  - CoBIT
  - IT Control Objectives for Sarbanes-Oxley
  - IT Governance Institute – [www.itgi.org](http://www.itgi.org)
    - Board Briefing on IT Governance
    - Board Briefing on Information Security



## Key Players (cont.)

---

- National Institute of Standards and Technology (NIST) – ([csrc.nist.gov](http://csrc.nist.gov))
  - Referenced in FFIEC Information Security Handbook
  - Referenced in key professional references
  - Lots of good reference stuff
    - Incident Response
    - Information Classification
    - Configuration Management (relies on NSA)



# Toys your IT people or person should become familiar with

---

- Center for Internet Security ([www.cisecurity.org](http://www.cisecurity.org)) has configuration baselines and automated scanning tool that can be used to test operating system security – including routers. Benchmark tool developed by recognized experts.
- The Nessus Project ([www.nessus.org](http://www.nessus.org)) – open source software tool that can be used to scan for network (including firewall) vulnerabilities.



## Other Players (cont)

---

- CERT ([www.cert.org](http://www.cert.org)) is a government sponsored research facility that is part of the software engineering institute at Carnegie Mellon University. Provides excellent reference tools.
- SANS ([www.sans.org](http://www.sans.org)) is a training organization which shares various white papers and other security awareness programs.

# WHILE YOU'VE BEEN SOX'd – THE FFIEC'S BEEN ISSUING



# HEADACHE RISK ASSESSMENT

FFIEC IT EXAM HANDBOOK	HEADACHE FACTOR	COMMENTS
Security	<b>Very High but getting better</b>	Banks are appreciating this more.... But there is just so much to do.
Outsourcing	<b>Very High</b>	Not issued yet...Anticipation. Hints from other handbooks indicate that this is destined to be a classic!
IT Audit	Moderate	Say goodbye to the one week, one size fits all IT general controls review.
eBanking	<b>High</b>	A mini-audit of the entire bank that considers most of the other exam handbooks.
BCP	Low	Procedures are not that bad – it's getting the business people involved that's the challenge
Retail Payments	Moderate	In the ballpark



# So – What's Different

---

- Beginning in very late 2002 (January 2003 to be exact), the FFIEC began issuing the new IT Exam Handbook Series
- These handbooks are gaining recognition as key references and reflective of “good” practices
- As a general IT audit guide, these handbooks are gaining recognition of “best practices”
- Processed-based audit approach could be major disadvantage for those banks not “believing” in documentation
- The 1-2 week general IT controls review is a thing of the past.



# Processed Based Approach

- Does the Board provide strategic direction and oversight?
  - *Yes, I realize it's IT – but they will need to get involved!!!*
  - *If needed, show them the questions to “the test.”*
  - *We'll review the 10 questions they should ask about security*
- Do you have a policy that communicates expectations and standards?
  - *Don't waste your time copying the “apple pie” policies that are in some books – specific accountabilities and procedures need to be communicated!!!*
  - *Use policies (and appendixes) to justify positions that may be different from those of the “intelligencia.”*
    - Changing passwords every 30 days vs. less frequent changes but more difficult passwords.
- Do you perform risk assessments or control self assessments to proactively identify issues?
  - *Don't wait for some outside party (e.g., regulator or auditor) to come in to tell you what is wrong.*
  - *Develop a “game plan” to fix high risk items and justify why you may not be able to get to low risk items.*
  - *SWAT Team to self-assess each FFIEC IT Exam Handbook as they are issued*

# Processed Based Approach (cont.)



- Do you have configuration guidelines (policies) for your technical platforms or do you just “trust your mechanic when you bring your car in?”
  - *Leverage information from the key players to jumpstart efforts and understand configuration options*
    - *NIST (routers and firewalls)*
    - *NSA (operating systems)*



# The 10 Questions Boards Should Ask About Security

*Source: Information Security Governance: What Directors Need to Know*

- What management system have we established to assure effective **assignment of accountability** for the security of our information and supporting technology resources?
  - *Management is responsible and the board accountable*
- What has management done to assure that all **parties know, understand, and accept** the importance of adhering to sound information security?
  - *Security awareness starts with the board and permeates the organization*
- What has management done to assure that we are **using our information assets** and administering information security in an ethical manner?
  - *Codes of conduct are followed in the use of computers as in other activities*



# The 10 Questions Boards Should Ask About Security (cont.)

---

- What has management done to assure that the perspectives and **considerations of all interested and affected parties** are considered and balanced in developing our information security policy?
  - *Security achieved through combined efforts of all and mindful of all participants*
- What **cost/benefit, risk, and due care analyses** have been applied to the selection of our information security controls?
  - *Security decisions made as others – management recommends and the board concurs*
- How has management coordinated and integrated information security with our **overall policies and procedures** to create and maintain effective security throughout our information systems?
  - *Security must be integrated into all relevant organizational policies*
- What capabilities do we have to assure that **failures involving information technology** or its management will not endanger the organization, its supported business units, its neighbors, or their information assets, and will not impair their ability to operate? (Consider requirements for timeliness, availability, and reliability.)
  - *As other risks, mitigate based on cost-effectiveness (and risk assessment)*

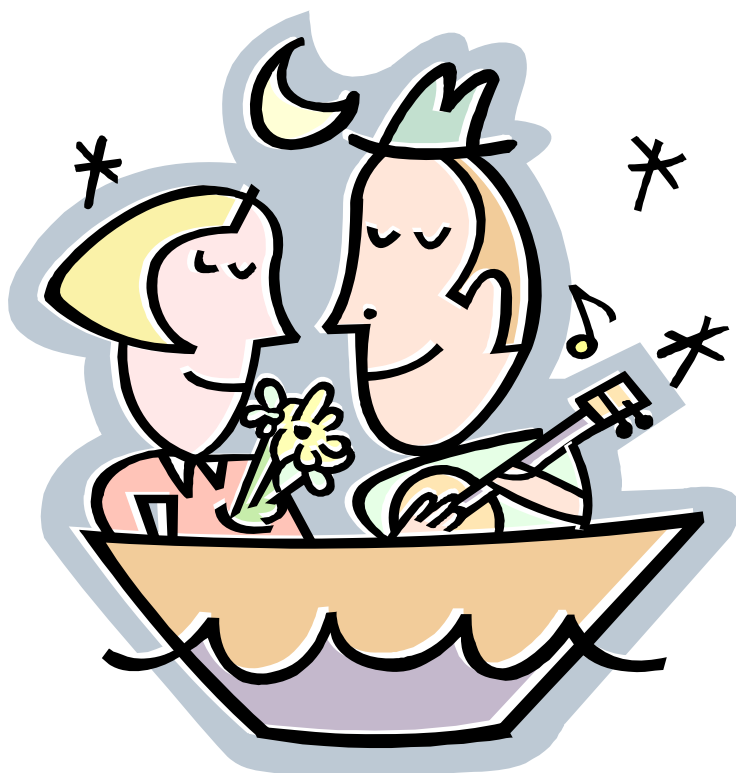


# The 10 Questions Boards Should Ask About Security (cont.)

---

- What capabilities do we have to assure that risks associated with information and supporting technology resources are **effectively assessed on an appropriate periodic basis**, or as otherwise required, and managed accordingly?
  - *Require periodic reporting by management and independent assessments by audit*
- How does management assure that our information **security measures are fair and legal**?
  - *Coordinate with the audit committee who are typically responsible for these issues*
- How effectively does management **share appropriate information with our peer organizations** and appropriate governmental entities?
  - *Get a plan together based on current practices and reviewed by relevant functions (e.g., legal, marketing, customer relationship, etc.)*

# Joel, we don't need to worry we outsource!!!!



- Is the love you feel for your information technology vendor “blinding” you to the business risks that you need to address?



# Then it's time for a risk management intervention!!!!

---

- Are you getting what you paid for?
- Do you know where your data is going?
- Will your vendor be there when you need them to be?
- Will the vendor's products/services help you comply with regulatory expectations?
  - Including "examination questions" that may not be officially part of a regulation.



# If Your Vendor Only Gives You Five Minutes Worth of Questions

---

- Do you have a SAS 70, and if so, is it a Type II report and what type of exceptions does it contain?
- How does your technology offering help my bank comply with regulatory/privacy expectations?
- Do you have an independent internal audit function and are they sufficiently staffed and qualified to identify problems at an early stage?
- How good is your insurance coverage and how does it protect my organization?
- Would my bank extend credit or invest in the vendor?



## A Good Contract Is The Foundation to Successfully Managing IT Vendor Risk

---

- Obtain legal counsel from an attorney familiar with similar transactions
  - Most companies use their general purpose corporate attorneys
  - Consider setting attorney's scope to go beyond simple contract language review
  - Confirm compliance with key industry or regulatory practices – many of which can be identified through basic research on the internet – and yes – the FFIEC Handbooks



# Structuring the Agreement

---

- Contract Flexibility
- Standards, Control and Regulatory Compliance
- Areas Outsourced/Purchased
- Financial Considerations
- Cost Savings (if premise for the transaction)
- Supplier Stability and Quality
- Management Fit
- Conversion Management



# Right To Audit Clauses

---

- They are not created equally
- Even if you have an airtight one – still may be impractical to audit
- What exactly are you allowed to audit
  - Compliance with contracted services
  - Controls over process to deliver service
  - Controls over billing process
  - How costs were determined
  - Anticipated or actual scope limitations
  - Time limitations – especially after “divorce” or contract termination
  - Vendor’s service providers and any sub-contractors
  - Unlimited right or does “cause” need to be shown

# Prioritizing Vendor Activities by Risk

<i>Perceived Risk</i>	<i>Percentage of Vendors</i>	<i>Percentage of Effort</i>	<i>Applicable References</i>
HIGH	5-10%	80%	Software Engineering Institute BITS
MEDIUM	10-20%	15%	CoBIT DoD Contractor Fraud Handbook
LOW	10-90%	5%	Relevant articles and generic workprograms (e.g., contract compliance and payables)

# Determining Perceived Risk – One Sample Approach

ISSUE TO CONSIDER	ITV RISK IS CONSIDERED LOWER	ITV RISK IS CONSIDERED AVERAGE	ITV RISK IS CONSIDERED HIGHER	WEIGHT	SCORE
The business line served by the ITV is (risk based on FFIEC Supervision of Technology Service Providers Handbook):	Bill Payment Services Check Processing Imaging and Electronic Safekeeping Web Site Hosting (Informational)	ACH Processing ATM/POS Processing and Switching Asset/Liability Management Credit Scoring Loan and Mortgage Processing Investment Processing Transactional Web Site Hosting	Asset Management Processing Clearing and Settlement Core Bank Processing Disaster Recovery Services		
Does ITV have access to confidential customer information	No	Yes but not enough to steal identity.	Yes		
SAS 70 and Other Third Party Reports	AICPA Trust Services Unqualified Opinion Provided	SAS 70 Type II Unqualified Opinion	No SAS 70, SAS 70 Type I or any Qualified Opinion		
ITV has an Internal Audit Department	Yes and personnel are qualified and relevant audits performed.	Yes – but “some” exceptions as to qualifications or relevancy.	No or “major” exceptions as to qualifications or relevancy.		



# Saved by a SAS 70?

---

- *...it has successfully issued its SAS No. 70 Type 1 report.... The self-initiated audit demonstrates...commitment to its customers as a reliable, transparent, secure ASP that is focused upon minimizing risk, increasing value, maintaining service availability, and preserving client privacy and data security.*
- *...is built on a foundation of values, and two of our most important values are integrity and "customer first." Earning a SAS No. 70 Type 1 certification [demonstrates our] acting on both of these values.*
- *Protecting customer data is the cornerstone of...success. Our SAS No. 70 audit is an important way to independently validate how well we manage...security.*
- *...passing the SAS No. 70...Type I audit is a key requirement for companies who wish to perform data-center and Web-hosting functions for financial...or other security-sensitive or regulated organizations. Such institutions can't use...firms that haven't passed the SAS No. 70 audit.*



# Not According to the AICPA!

---

- “The guidance in SAS No. 70, Service Organizations, as amended, is applicable to the audit of the financial statements of an entity that obtains services from another organization that are part of the user organization’s information system.”



# Incorporating SAS 70 into a IT Vendor Management Program

---

- Managers and their auditors (both internal and external) should discuss the need to actually review the report.
- At a minimum, the report could provide risk managers with a good source of background information on the vendor.
- Review vendor management policy describing the need, if any, for various departments to review the SAS No. 70.
- The opinion within the SAS No. 70 report will clarify whether it is a Type I or Type II report.
  - Type I – Identified Controls Tested
  - Type II – Identified Controls Not Tested
- The report section entitled “The Service Organization’s Description of Controls” enables the vendor to provide background information that it deems to be important to readers. This section is generally not audited by the auditor and should be treated as such.
- The next section, “Information Provided by the Service Auditor,” provides additional details about the suitability of controls identified to support the control objectives.
  - In a Type II report, the auditor tests the effectiveness of these controls. Because the *vendor* and not the *auditor* specifies the control objectives being reported on, potential weaknesses can be identified by noting the types of control objectives normally associated with the given process that are *not* included.
- Finally, “User Control Considerations,” normally a one-to two-page section of the report, is a must-read for all. This section identifies those controls identified by the service auditor that are the responsibility of the customer.



# AICPA Introduces Trust Services

---

- Includes SysTrust, WebTrust and Privacy Framework.
- Perhaps the greatest difference between the new services and the previous SAS No. 70 is that, instead of having the vendor identify which control objectives should be tested, the objectives are tested against predetermined criteria and illustrations that have been subject to due process procedures, including exposure of the proposed criteria for public comments. This results in an expressed opinion as to whether the vendor complies with the criteria.
- However, since these new services set a higher standard, the vendor is not likely to volunteer for the additional scrutiny.
- Alternatively, other forms of assurance could be developed to ensure vendor compliance with other standards, such as those published by the FFIEC, BITS or other reputable organizations.



# “Good” Practices

---

- Be careful “whom you marry” (due diligence)
- Document ALL expectations – including getting a “pre-nup” agreement
- Assign accountable executive – both for service delivery and cost of service
- Develop contract extracts (in english) so that “the team” knows the rules
- Measure and monitor what’s important
- Trust but verify (use the audit clauses)
- Implement “fraud prevention” program (to catch honest mistakes)
- Exercise prudent business judgement



# Good Banks Gone Bad – From an IT Risk Management Perspective

---

- Board not providing appropriate oversight.
- Ignoring audit report comments.
- MIS doesn't produce the data needed to monitor or review loans or investments.
- Not taking GLBA seriously.
- "Feeble" efforts at a technology risk assessment or not following up on issues.
- Not proactively managing security.
- Not appropriately managing vendors.



# Staying In Touch with Joel

---

- Contact Joel directly at:  
Joel Lanz  
Joel Lanz, CPA, P.C.  
P.O. Box 597  
Jericho, NY 11753-0597  
(516) 933-3662  
[jlanz@bankingcpa.com](mailto:jlanz@bankingcpa.com)
- Visit [www. bankingcpa.com](http://www.bankingcpa.com) for upcoming vendor management related articles:
- "Managing IT Outsourcing Risks" (Journal of Accountancy – June 2004 Tentative Date).
- "Incorporating SAS No. 70 and Other Reports into a Vendor Management Program" (The RMA Journal – April 2004).
- "Unmasking IT Fraud: Practical Applications of SAS-99" (Bank Accounting & Finance – April 2004)
- "Five Must Ask Outsourcing Due Diligence Questions" (Western Banker – January 2004)