

---

# CONDUCTING A SECURITY RISK ASSESSMENT

## PHOCUS 2003

---

Joel Lanz, CPA, CISA, CISSP.

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

[jlantz@itriskmgt.com](mailto:jlantz@itriskmgt.com)

---

WHAT WILL WE BE TALKING ABOUT  
TODAY AND IN WHAT LEVEL OF DETAIL?



---

# YOUR HOST

- 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 IS IT GOVERNANCE?



---

# Unprecedented Guidance

- National Association of Corporate Directors
    - Information Security Oversight: Essential Board Practices
  - Institute of Internal Auditors and the Critical Infrastructure Assurance Project (includes NACD, IIA, ISACA and AICPA)
    - Information Security Governance: What Directors Need to Know
  - IT Governance Institute (Information Systems Audit and Control Association)
    - Board Briefing on IT Governance
  - *AND DON'T FORGET EVOLVING SARBANES-OXLEY GUIDANCE*
-

---

# The 10 Questions Boards Should Ask

- What management system have we established to assure effective **assignment of accountability** for the security of our information and supporting technology resources?
- What has management done to assure that all **parties know, understand, and accept** the importance of adhering to sound information security?
- What has management done to assure that we are **using our information assets** and administering information security in an ethical manner?
- 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?
- What **cost/benefit, risk, and due care analyses** have been applied to the selection of our information security controls?
- How has management coordinated and integrated information security with our **overall policies and procedures** to create and maintain effective security throughout our information systems?
- 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.)
- 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?
- How does management assure that our information **security measures are fair and legal**?
- How effectively does management **share appropriate information with our peer organizations** and appropriate governmental entities?

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

---

---

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
-

---

# HOW DO YOU PERFORM A TECHNOLOGY RISK ASSESSMENT?

---

---

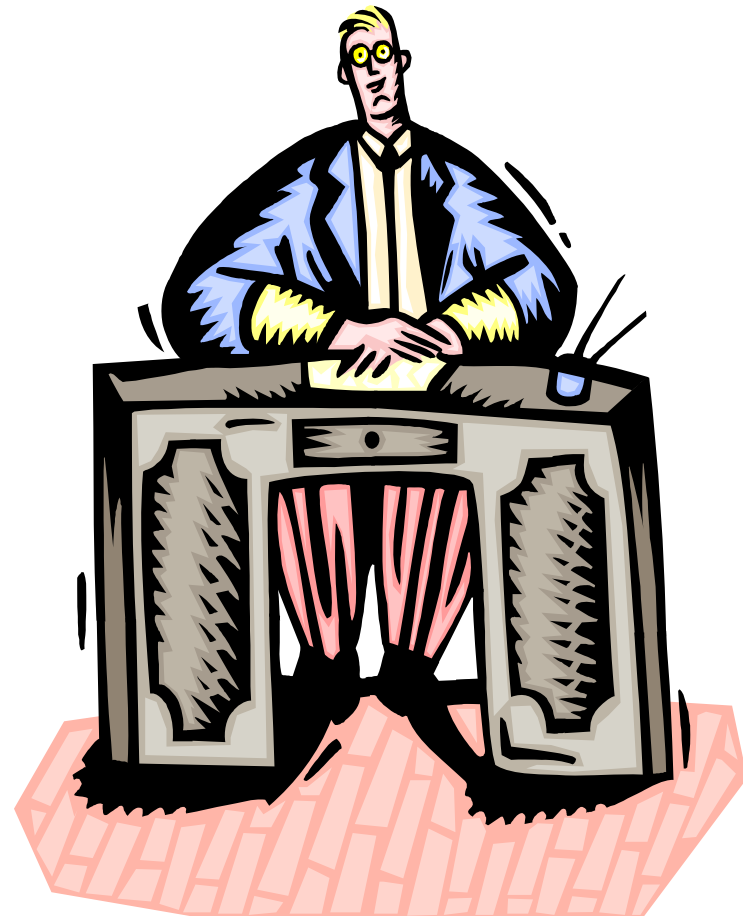
# But first.....why perform?

- Regulatory expectation
  - Need to cost-effectively mitigate technology-related operational risk in an ever more complex and pressured environment.
  - Many organizations face multiple high-priority items – for example which do you do first?
    - Ensuring high level of security
    - Implement new systems quickly to capture competitive advantage
    - Increase ROI on technology investments
  - Unlike financial risk, technology risk can't be easily quantified or measured.
-

---

# So what - I'm still not convinced!!!

- Proactively identify vulnerabilities
- Align risk-management activities with business imperatives
- Efficiently use corporate risk management resources
- Ensure cost-effective control environment



---

# Team Approach Between Users, IT and Internal Audit

- Gather and confirm understanding
  - Identify and define threats
  - Develop a vulnerability inventory
  - Translate technical vulnerabilities into business vulnerabilities
  - Determine probability and exposure
  - Rank issues
  - Develop recommendations and discuss with management
  - *Source: NIST Special Publication 800-30, "Risk Management Guide for Information Technology Systems."*
-

---

# Where To Begin?

- Leverage established standards and methodologies as identified by the ABA
    - ❑ COBIT
    - ❑ ISO Standards
    - ❑ NIST
    - ❑ OCTAVE
    - ❑ Trust Services
  - Other standards and methodologies
  - Test through vulnerability assessment and penetration testing
-

---

# COBIT

- Sponsored and funded by the IT Governance Institute (affiliate of the Information Systems Audit and Control Association)
  - Consists of a framework of IT processes and control objectives that can be implemented to control, audit and manage the IT organization
  - Framework emphasizes best practices and leverages other recognized methodologies and tools such as COSO, ISO, ITIL, NIST and AICPA.
  - Focus is on helping leaders understand and manage the risks relating to IT and the links between the management process, the technical questions, the need for control and the risks
  - Proposed as a first step to avoid confusion with various other guidelines and methodologies
  - Attempts to provide an integrated methodology for management, users and auditors
-

---

# COBIT

- Contains 34 High-Level Control Objectives within 4 Domains
    - Planning and Organization
    - Acquisition & Implementation
    - Delivery & Support
    - Monitoring
  - 318 Detailed Control Objectives
  - Management guidelines for each of the control objectives:
    - Critical Success Factors
    - Key Goal Indicators
    - Key Performance Indicators
    - Maturity Model Definitions
  - Audit guidelines that leverage a generic IT audit template:
    - Obtain an understanding
    - Evaluate the controls
    - Assess compliance
    - Substantiate the risk
-

---

# COBIT

## PROS

- Well respected and recognized tool - even by regulators
- Excellent methodology for getting various parts of an organization to speak the same language
- Looks at IT in general - not just security
- Facilitates communication with top level executives
- Excellent senior management perspective (e.g., CMM, CSFs)
- Small business version coming out this year

## CONS

- Current supporters are primarily in the IT audit community
  - More of a general assessment tool - detailed issues to consider are in the form of audit programs
  - Some practitioners consider it to be too burdensome or theoretical - yet, it has received the support of many organizations
  - Can be burdensome to very small banks – however, release of a small business version is imminent.
-

---

# ISO

- ISO (the International Organization for Standardization) along with the International Electrotechnical Commission) form the specialized system for worldwide standardization.
  - The stated purpose of ISO 17799 is to “provide a common basis for developing organizational security standards and effective security management practice and to provide confidence in inter-organizational dealings.”
  - Originally developed in Britain, the standard has gained much popularity and is a favored TRA approach in Europe. It is typically used in larger organizations especially those involved with international activities. The standard is often referenced and leveraged by other prominent methodologies.
  - Very specific guidance that requires specific modification and adaptation
  - Leveraged by other well-known methodologies
-

---

# ISO

- Security Policy
  - Communications and Operations Mgt.
  - Organizational Security
  - Access Control
  - Asset Classification and Control
  - System Development and Maintenance
  - Personnel Security
  - Business Continuity Management
  - Physical and Environment Security
  - Compliance
-

---

# ISO

## Pros

- Very detailed guidance
- Ten focus areas
- Standard of Standards
- Common language
- Well known
- Favored by large business partners (e.g., insurance carrier or large CPA firm)

## Cons

- Overkill for most banks
  - Few “free” tools to leverage
  - Strict copyright policy
  - Last updated in 2000
  - Imperfections identified by US/Canadian government standard setting groups
-

---

# NIST

- Guidance comes from the Information Technology Laboratory (“ITL”) which provides leadership for the nation’s measurement and standards infrastructure.
  - ITL develops technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in federal computer systems.
  - Publications issued report on ITL’s research, guidance, and outreach efforts in computer security, and its collaborative activities with industry, government and academic organizations.
  - As governmental agencies, banking regulators frequently participate in NIST research and are audited against these guidelines.
  - Many other methodologies leverage the work performed by the NIST.
-

---

# NIST

- Like the other organizations mentioned previously, NIST provides a detailed checklist of IT-related risk mitigation strategies that should be assessed as part of a TRA. This checklist is contained in NIST Special Publication 800-26 – “Security Self-Assessment Guide for Information Technology Systems.”
  - In addition to its detailed coverage of security issues, the checklist provides the ability to enable the TRA team to determine if risk is managed by using five “levels of effectiveness” which follows:
    - Level 1 – control objectives documented in a security policy
    - Level 2 – security controls documented as procedures
    - Level 3 - procedures have been implemented
    - Level 4 – procedures and security controls are tested and reviewed
    - Level 5 – procedures and security controls are fully integrated into a comprehensive program
-

---

# NIST

## PROS

- Very detailed guidance
- Leveraged by other methodology organizations and professional associations - "Thought Leadership"
- Most recently issued guidance on security risk assessment (Fall 2001-current)
- Facilitates distribution of instructions and development of policies
- Used internally by regulatory agencies (e.g., used by federal agencies)

## CONS

- Geared for the security of government agencies
  - "Blind" following of the methodologies could be too burdensome in a smaller organization
  - Could be considered "excessive" for those primarily concerned about satisfying external reviewer needs only
-

---

# OCTAVE

- Developed by the Software Engineering Institute (SEI) at Carnegie Mellon University, OCTAVE is a comprehensive self-directed approach to TRA.
  - It differs from traditional TRAs in that it first determines what information assets really need to be protected and then evaluates the technology infrastructure to determine the vulnerability of those assets.
  - The SEI is home to The CERT Coordination Center (CERT/CC) a center of respected computer expertise and distributor of CERT alerts and other information relating to managing security vulnerabilities.
  - The robustness of tools, workshops and publications relating to OCTAVE significantly enhances the effectiveness of the risk assessment.
-

---

# OCTAVE

- Uses a three-phased approach to identify the technology risk management needs of an enterprise:
    - Build Asset-Based Threat Profiles – includes the identification of important information assets, the threats to those assets, security and current risk mitigation strategies.
    - Identify Infrastructure Vulnerabilities – includes examining technology infrastructure for vulnerabilities that can be compromised.
    - Develop Security Strategy and Plans – Based on the result of the first two phases, develop a strategy based on business priorities to mitigate risks.
-

---

# OCTAVE

## PROS

- Comprehensive methodology
- Leverages combination of academic research and industry practices
- Superior pedigree and project sponsors
- Full methodology and supporting tools
- Small business version coming out this year

## CONS

- Currently geared to larger institutions (although a version for smaller organizations is planned).
  - Formal training in the use of the tool required by most users.
  - “Cooperative” approach may be too cumbersome for some organizations.
-

---

# TRUST SERVICES

- Assurance service provided by CPAs to increase comfort of management, board of directors, customers and business partners with the systems that support a business or particular activity
  - Focuses on high-level objectives relating to availability, security, integrity and maintainability
  - Intended as an adjunct product to more traditional SAS 70 reviews
  - Focuses on
    - Communicating performance objectives, policies and standards
    - Use of procedures, people, software, data and infrastructure
    - Monitoring activities
  - Combines former WebTrust and SysTrust services
  - Relatively new service – gaining momentum but still not very well known
-

---

# TRUST SERVICES

- Five stand-alone principles and criteria
    - Security
    - Availability
    - Processing
    - Online Privacy
    - Confidentiality
  - Organized into four broad areas:
    - Policies
    - Communications
    - Procedures
    - Monitoring
-

---

# TRUST SERVICES

## PROS

- Good high level questions that provides an overview on overall reliability
- Specific focus areas on security and privacy
- Facilitates communication with non-IT department
- Third-party opinion (CPA) available

## CONS

- Relatively new
  - Not detailed enough for intended objectives
  - More of an “executive-level” assessment perspective rather than “fix-it”
  - CPA practitioner community has not thrown full support behind this yet
-

---

# REGULATORY

- Cumulative guidance provided by the various banking regulatory agencies
  - Baseline guidance provided by 1996 FFIEC “Bluebook” which is generally recognized as being “batch processing” oriented
  - Guidance is being replaced with a new IT Examination booklet series
    - Information Security released at the end of January
  - Guidance supplemented by various “publications” issued during the past six years
  - Focus of material is on what needs to get done - starting to provide “high-level” suggestions on how to get it done
  - “Newer material” generally incorporates “best-practices”
  - 501(b) high-level catch all
-

---

# REGULATORY

## Representative Detailed Guidance and Methodologies

- IT Examination Booklet – Information Security
  - OTS Vendor Management
  - FFIEC 1996 Bluebook
  - 501(b) Exam Procedures (privacy)
  - Technology Outsourcing Information Documents
  - Network Security Vulnerabilities
  - Internet-Initiated ACH Transactions
  - Risk Assessment Tools and Practices for Information System Security
  - Security Risks Associated with the Internet
  - Internet Banking
-

---

# REGULATORY

## PROS

- Focuses on achieving the minimally acceptable standard
- Fair balance between detailed and general control concerns and procedures
- Popular method at many Banks - especially very small banks

## CONS

- Cumbersome series of questionnaires that need to be supplemented
  - A number of areas do not specify how to accomplish
  - Guidance can generally lag practices by 6 months - 2 years.
  - Moving targets
  - Piecemeal sources that need to be patched for comprehensiveness
  - What if guidance hasn't been released yet?
-

---

# And What About Consultant's Proprietary Methodologies?



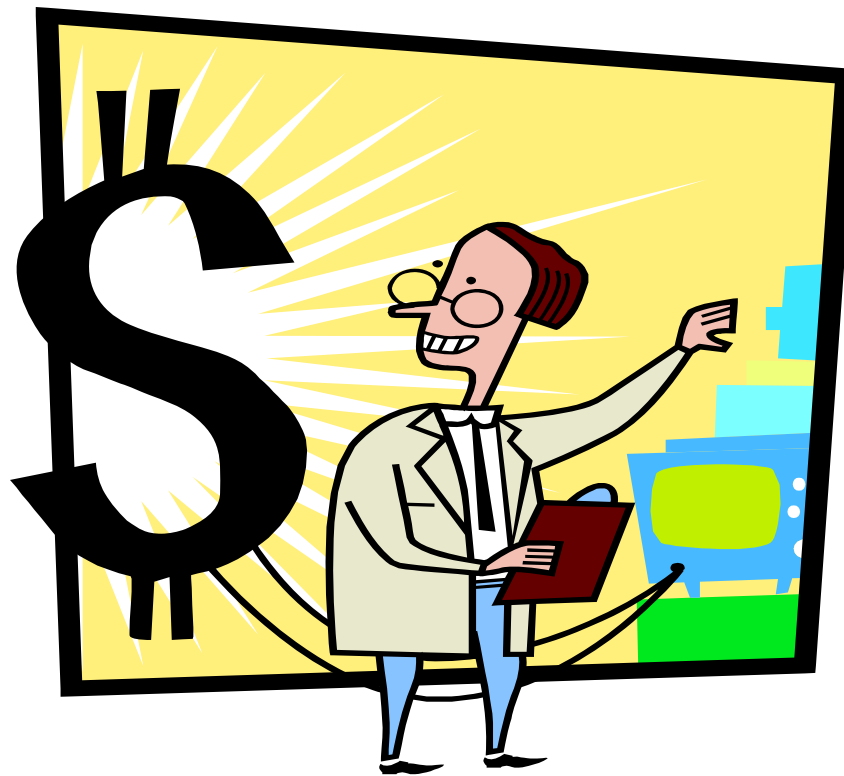
---

# Things to Think About

- How does the proprietary methodology leverage relevant standards?
  - Is the methodology complete, up to date and thorough?
  - What is the experience of those executing the methodology?
  - How does the consultant ensure compliance with their methodology?
  - Are you forever “married” to the consultant to do TRAs because of the use of a proprietary tool?
  - How does the methodology stack against current regulatory expectations?
  - Will the methodology enable you to proactively identify tomorrow’s issues?
-

---

# HOW DOES A PENETRATION TEST DIFFER FROM A VULNERABILITY ASSESSMENT ?



---

# How to get in with technical know-how?

- Misconfigured Routers
  - Unsecured/Unmonitored Remote Access
  - Excessive Trust Relationships
  - Accounts with Excessive Privileges
  - Unpatched, Outdated and “Default” Software
  - Poor Policies, Procedures & Guidelines
  - Excessive File & Directory Privileges
-

Why do they really get in most of the times?



---

# Vulnerability Assessments

## ■ WHAT IT IS

- ❑ Identifies not just hosts and open ports but any associated vulnerabilities automatically instead of relying on human interpretation of the results.

## ■ TYPICAL FINDINGS

- ❑ Upgrade or patch vulnerable systems
- ❑ Deploy mitigating strategies
- ❑ Tighten configuration management program
- ❑ Monitor vulnerability alerts and mailing lists and determine applicability to environment
- ❑ Modify security policies for updates and upgrades

## ■ ACTIONS

- ❑ Identify active hosts on a network
  - ❑ Identify active & vulnerable ports on hosts
  - ❑ Identify application and banner grabbing
  - ❑ Identify operating systems
  - ❑ Identify vulnerabilities associated with discovered operating systems and applications
  - ❑ Testing compliance with host application usage/security policies
  - ❑ Establishing a foundation for penetration testing
-

---

# Vulnerability Assessments (cont.)

## ■ STRENGTHS

- ❑ Fairly fast & efficient
- ❑ Some freeware tools available
- ❑ Highly automated for known vulnerabilities
- ❑ Often provides advice for mitigating strategies
- ❑ Easy to run regularly
- ❑ Cost varies by tool used

## ■ OTHER INFO

- ❑ Every 2-3 months
- ❑ High level of complexity and effort with medium risk

## ■ WEAKNESSES

- ❑ High false positive rate
- ❑ Large amount of network traffic
- ❑ Not stealthy (detected)
- ❑ Not for rookies
- ❑ Often misses new stuff
- ❑ Identifies the easy stuff

## ■ BENEFITS OF DOING

- ❑ Enumerates the network structure and what's active
  - ❑ Identifies vulnerabilities on a target set of computers
  - ❑ Validate up-to-date patches and software versions
-

---

# Penetration Testing

- WHAT IT IS

- A security test in which evaluators attempt to circumvent the security of a system based on their understanding of the system design and implementation by using common tools and techniques used by hackers.

- TYPICAL FINDINGS (Exploits)

- Kernel Flaws
- Buffer Overflows
- Symbolic Links
- Race Conditions
- File & Directory Permissions
- Trojans
- Social Engineering

- ACTIONS (“Rules of Engagement”)

- Specific IP address/ranges to be tested
  - Host not to be tested
  - A list of acceptable testing techniques and tools
  - Time that scanning is to be conducted
  - IP address of attack machine
  - Prevention of false alarms to law enforcement
  - Handling of information collected by the testing team
-

---

# Penetration Testing (cont.)

- **DISCOVERY PHASE**
    - footprinting, scanning and enumeration
  - **GAINING ACCESS**
    - Gather info to make an informed attempt at the target
  - **ESCLATING PRIVILEGE**
    - The tester seeks to gain additional privileges or rights
  - **SYSTEM BROWSING**
    - Pilfering: Attempt to gain access to trusted systems
  - **LEAVE BEHINDS**
    - Covering Tracks, Creating Back Doors
-

---

# Penetration Testing (cont.)

## ■ STRENGTHS

- ❑ Employ hacker “methodology”
- ❑ Goes beyond surface vulnerabilities to show how they can be exploited to gain access
- ❑ Shows that vulnerabilities are real
- ❑ Social engineering allows for testing of procedures and human reactions

## ■ OTHER INFO

- ❑ Annually
- ❑ High level of complexity, effort and risk

## ■ WEAKNESSES

- ❑ What’s a hacker “methodology”
- ❑ Requires great expertise – dangerous when conducted by rookies
- ❑ Due to time requirements not all resources tested individually
- ❑ Certain tools may be banned or controlled by regulations
- ❑ Legal complications and organizationally disruptive
- ❑ Expensive

## ■ BENEFITS OF DOING

- ❑ Determines how vulnerable and level of damage that can occur
  - ❑ Tests IT staff response and knowledge of security policies
-

---

# Don't Forget About Social Engineering

- “Are You the Weak Link,” Harvard Business Review, Mitnick, April 2003.
  - “The greatest misconception about security is that a computer is the hacker’s most dangerous tool. Not so. It’s the phone. As security technologies improve, attackers are resorting to old fashioned con games to get what they want. Why pound on the heavily defended corporate firewall when it’s easier to just trick the assistant who answers the phone into revealing his boss’s password”.
-

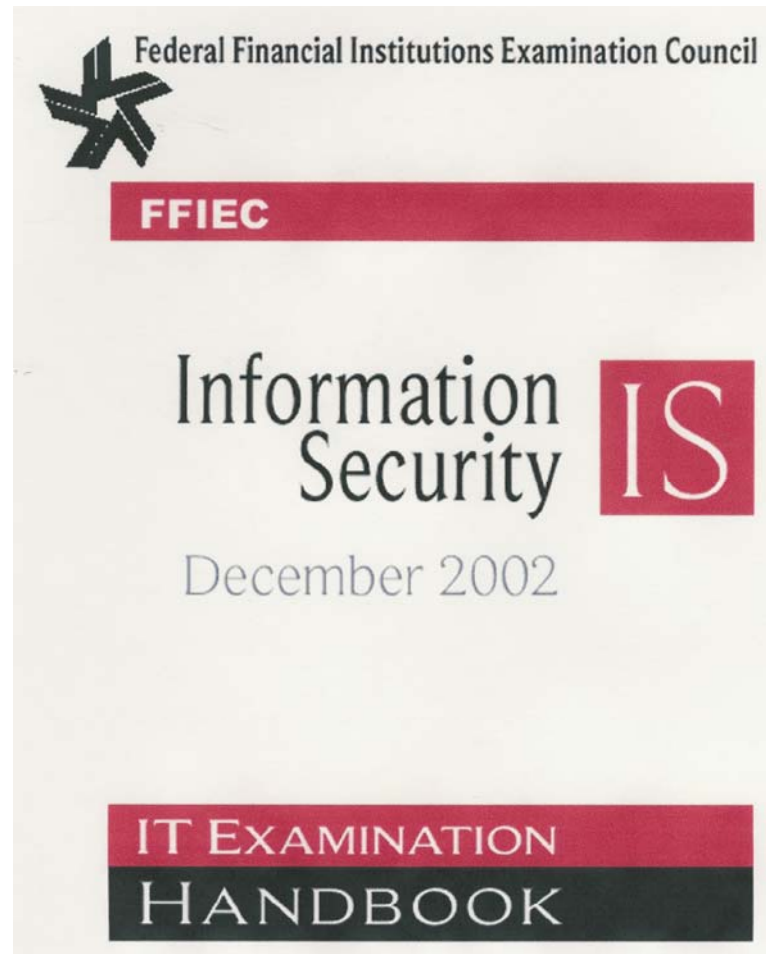
---

# 7<sup>th</sup> INNING STRETCH!!!!



---

# YOUR IMMEDIATE CONCERN



---

# TIER 1 Exam Procedures

- Determine the appropriate scope for the examination
  - Determine the complexity of the institution's information security environment
  - Determine the adequacy of the risk assessment process
  - Evaluate the adequacy of security policies relative to the risk to the institution
  - Evaluate the security-related controls embedded in vendor management
  - Determine the adequacy of security testing
  - Evaluate the effectiveness of enterprise-wide security administration
  - Discuss corrective action and communicate findings
-

---

# Some Thoughts.....

- Have you resolved all prior audit and examiner comments?
  - Are the basics (hardware/software) documented?
  - Who is leading the security efforts and are they qualified to do so?
  - Have you done a technology risk assessment – and if so, did you leverage a recognized standard or methodology? Is the assessment periodically updated?
  - How current are your IT-related policies and do you have what you need? Does everyone understand their responsibilities and “organizational ground rules?”
  - Is the security-related due diligence in vendor relationships sufficient?
  - Are you taking privacy seriously – spirit not just letter of the law?
  - What type of ongoing security testing do you perform?
  - What is the attitude toward security outside the IT Department?
  - BUSINESS Continuity Plans updated?
-

---

# And if you know everything here are the TIER 2 Exam Procedure Topics

- Authentication and Access Controls
  - Network Security
  - Host Security
  - User Equipment Security (Laptop/Wireless)
  - Physical Security
  - Personnel Security
  - Application Security
  - Software Development and Acquisition
  - Business Continuity – Security
  - Intrusion Detection and Response
  - Service Provider Oversight – Security
  - Encryption
  - Data Security (e.g., protection of information)
-

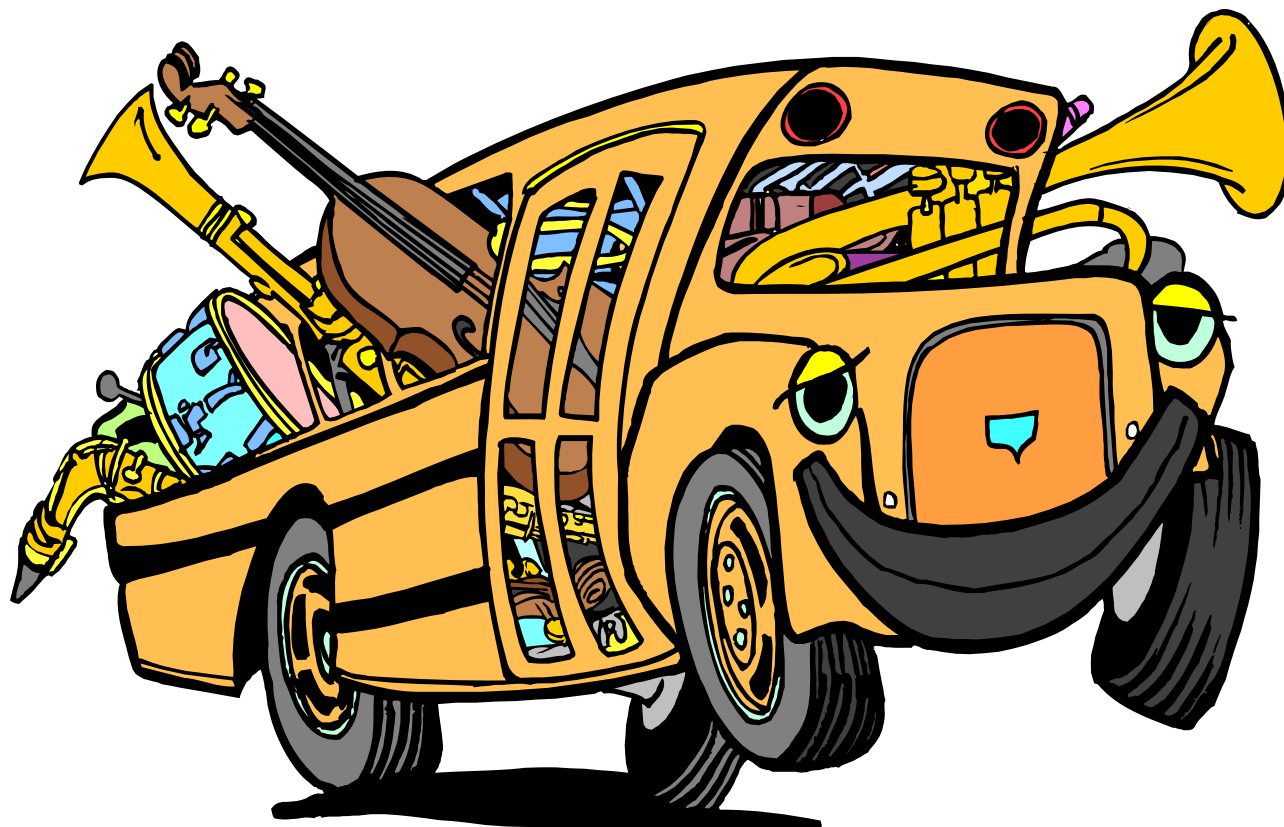
---

## With More Handbooks to Come

- Audit
  - Business Continuity Planning
  - Development and Acquisition
  - Electronic Banking
  - Management
  - Operations
  - Outsourcing
  - Payment Systems
  - Supervision of Technology Service Providers
-

---

WHAT DOES THIS ALL MEAN FOR  
THE COMMUNITY BANKER?



---

# Does management learn what they need to know about IT to manage responsibly?

- “The iPremier Company: Denial of Service Attack,”  
Harvard Business School Case # 601-114
  - The case is primarily intended to:
    - provide an opportunity to explore crisis management issues in the modern context of computer security
    - make the point that general managers cannot leave infrastructure management entirely to their technical staffs
    - Demonstrate that technical issues are closely intertwined with business issues when it comes to internet security
-

---

# Common High Priority Areas for the Average Community Bank

- Board involvement with technology
    - Answering questions that NACD, IIA, AICPA and ISACA believe directors should be asking
  - Policies, Procedures and Guidelines
    - Focusing on “position” and “department” roles and responsibilities
  - Security Hardening Guidelines
    - Leveraging vendor guidelines, technical audit programs and industry consensus guidelines
  - Vendor Management Programs
    - Using BITS framework and communicating expectations
  - Manage Customer Data
    - Considering the spirit and not just the letter of the law or expectation
  - Electronic Communication Management
    - Managing the impact of wireless, laptop, handhelds, email, voice mail – not just from a security perspective – but also customer confidentiality
  - Incident Response Plans
    - Just in case – media and law enforcement relations and what actions to take
-

---

# Challenges to Overcome

- Integrating these efforts with other corporate governance initiatives
  - Choosing the “appropriate” TRA methodology and getting stakeholder buy-in
  - Understanding that TRA is the first step – risk mitigation is also required
  - Keeping the assessment up to date
  - Developing or enhancing policies for TRA and Data Classification
  - Are you aiming for “best practice” or “acceptable practice”
  - Finding the time
-

---

# REGULATORY GUIDANCE, RESOURCES AND STANDARDS

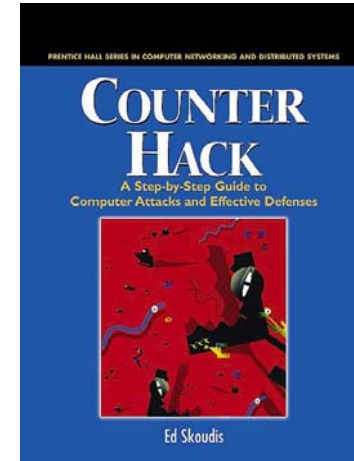
- See Page 3 of the new examination handbook
  - Banks have a variety of resources to draw upon
    - Federal laws and regulations
    - Third-party or security industry resources
    - National and international standard-setting organizations
  - “While no formal industry accepted security standards exist, these various standards provide benchmarks that both financial institutions and their regulators can draw upon for the development of industry expectations and security practices. Some standard-setting groups include the following organizations:
    - NIST
    - ISO
    - ISACA’s COBIT
-

---

# What Joel is Recommending to his Clients

- Use a combination of tools/methodology from NIST and COBIT:
    - NIST
      - Overall project methodology (including risk determination)
      - Detailed self-assessment questionnaire that allows analysis that corresponds to the examination handbook as well as COSO (for Sarbanes) activities
        - Policies/Strategies
        - Documented Procedure
        - Monitoring
        - Periodic Testing
    - COBIT
      - High level control objectives used to consolidate findings and prioritize into manageable tasks
      - Detailed control objectives used to identify areas for improvement
      - Management guidelines used to provide comparison against others using an established and recognized maturity grid.
      - Small business COBIT scheduled for release soon
  - See what happens with ISO and the new BS 7779 standard
-

# SUMMER & VACATION READING



MORE THAN ONE MILLION COPIES SOLD!

*"Gerber's powerful insights have given thousands of entrepreneurs new control over their businesses..."*  
—Success Magazine

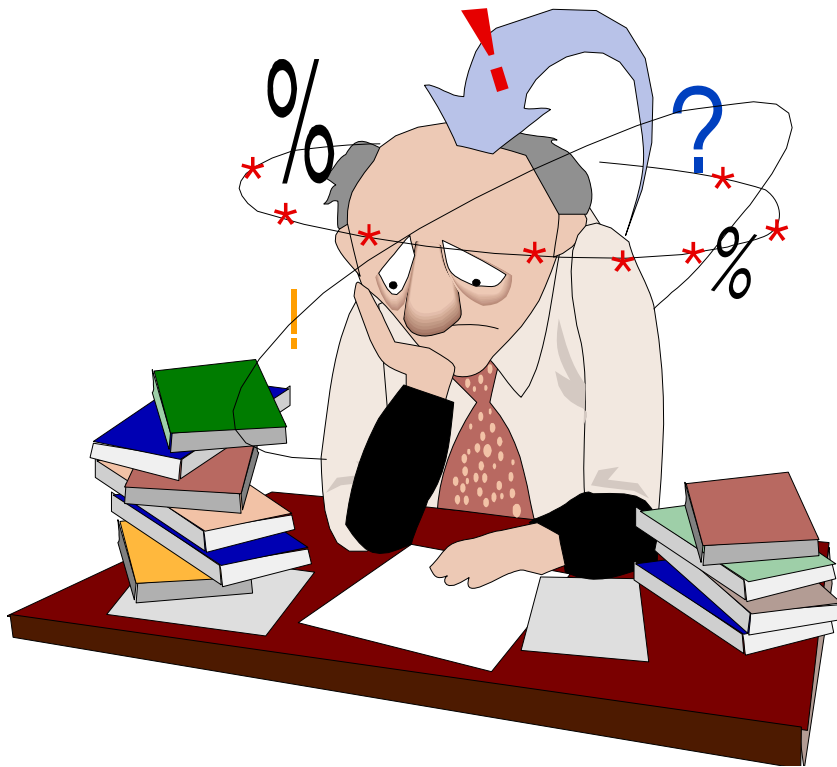
**The E Myth**  
**Revisited**

Why Most Small  
Businesses Don't Work  
and What to Do About It

**MICHAEL E. GERBER**  
Author of the Bestselling Classic *THE E-MYTH*

---

# 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

---