

---

# ENHANCING TECHNOLOGY GOVERNANCE SKILLS

(TO GET YOU PAST THE VELVET ROPES AT CLUBS  
AROUND TOWN)

---

12<sup>TH</sup> Annual Conference  
The Institute of Internal Auditors  
Long Island Chapter

---

# ADMINISTRATION

- Three hour session with a 20 minute break.
  - Please complete “IIA paperwork” to ensure proper crediting of CPEs.
  - Handouts include:
    - Copies of slides
    - Two recent published articles by the speaker:
      - “Prioritizing Aspects of Technology Risk Assessment and Mitigation.”
      - “Practical Aspects of Vulnerability Assessment and Penetration Testing.”
      - Client newsletter describing regulatory security changes
-

---

# COCKTAIL PARTY QUESTIONS

- What will we be talking about today and in what level of detail?
  - What is IT Governance?
  - How do you perform a Technology Risk Assessment?
  - How does a penetration test differ from a vulnerability assessment?
  - 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 should 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?
  - What does this all mean for the Internal Auditor?
-

---

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



---

# WHAT IS IT GOVERNANCE?

---

# Unprecedented Guidance

National Association  
of Corporate Directors®



Board Leadership Series

## Information Security Oversight Essential Board Practices

December 2001

Published by  
The National Association of Corporate Directors®

Sponsored by  
KPMG's Audit Committee Institute

In collaboration with  
The Institute of Internal Auditors  
and  
The Critical Infrastructure Assurance Office,  
U.S. Department of Commerce



“IT governance is the term used to describe how those persons entrusted with governance of an entity will monitor IT in their operations, including control and direction of the entity. How IT is applied within the entity will have an immense impact on whether the entity will attain its vision, mission or strategic goals.”

— Robert J. Korman, CPA, Nonprofit,  
Director of Institute Governance

“The board of directors of my company is well aware its role is to oversee the company's operational strategies, structures, systems, staff and standards. However, as president of the company it is my responsibility to ensure that they extend that oversight to the company's IT as well. In today's economy, and with our reliance on IT for competitive advantage, we might as well afford to apply to our IT anything less than the level of commitment we apply to overall governance.”

— Michael Cardinal, Director and Chair, Directors' Council,  
Director, Global Green Inc.



The IIA The Institute of Internal Auditors  
Critical Infrastructure Assurance Project

## Information Security Governance: What Directors Need to Know

*“Just as an audit committee does no auditing, a board of directors cannot provide information security. But by asking trenchant questions and insisting on clear, responsible answers, the board can provide a level of needed oversight to this vital business function that is adequate and necessary, and in doing so, exercise its essential duty of care.”*

-- Thomas Horton, Chairman, National Association of Corporate Directors

# 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?*

---

# 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
-

---

# HOW DO YOU PERFORM A TECHNOLOGY RISK ASSESSMENT?

---

---

# Handout # 1

- “Prioritizing Aspects of Technology Risk Assessment and Mitigation”
    - Published in the December 2002 edition of Bank Accounting and Finance.
-

---

# But first.....why perform?

- 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."*
-

---

# How to develop a vulnerability inventory?

- Leverage established standards and methodologies
    - CoBIT
    - eSAC
    - ISO Standards
    - NIST
    - Octave
    - Trust Services
  - Test through vulnerability assessment and penetration testing
-

---

HOW DOES A PENETRATION TEST  
DIFFER FROM A VULNERABILITY  
ASSESSMENT ?

---

---

## Handout # 2

- “Practical Aspects of Vulnerability Assessment and Penetration Testing”
  - Published in the February 2003 edition of The RMA Journal.



---

# 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
-

---

# 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(es) 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
-

---

# The Practical Auditor

- Vulnerability assessment is a management control that should be performed frequently
  - Management should follow-up on the vulnerabilities identified and reconcile to actions taken
  - Where necessary, compensating controls should be implemented
  - Auditors should perform compliance testing on the above controls
-

---

## But Joel, you don't understand the reality of our corporate environment

- If audit doesn't do it – it will not get done
  - Too much to do – too few resources
  - The Techies don't appreciate the need for security
  - The highest authorities expect that we do it
  - We need to show them that it is wrong or else they will not take action
  - What else will our IT auditor do
-

# Wrong Answer!!!

**EXPOSURE DRAFT**

**PROPOSED STATEMENT ON AUDITING STANDARDS**

**Communication of Internal Control Related Matters Noted in an Audit**

**March 18, 2003**

Prepared by the AICPA Auditing Standards Board for comment from persons interested in auditing and reporting issues

Comments should be sent via the Internet to Julie Anne Dilley at [jdilley@aicpa.org](mailto:jdilley@aicpa.org) and received by May 30, 2003



Federal Register

Thursday,  
February 20, 2003


**Part II**

**Department of Health and Human Services**

Office of the Secretary

45 CFR Parts 160, 162, and 164  
Health Insurance Reform Security Standards; Final Rule

Federal Financial Institutions Examination Council



**FFIEC**

Information Security **IS**

December 2002

**IT EXAMINATION HANDBOOK**

H. R. 3763

**One Hundred Seventh Congress  
of the  
United States of America**

**AT THE SECOND SESSION**

*Began and held at the City of Washington on Wednesday,  
the thirtieth day of January, two thousand and two*

**In It**

To provide a means for improving the accuracy and reliability of corporate disclosures made pursuant to the Securities Exchange Act of 1934 and the Securities Exchange Act of 1933.

It is enacted by the Senate and House of Representatives of the United States of America in Congress assembled,  
**SECTION 101. SHORT TITLE.—**This Act may be cited as the "Sarbanes-Oxley Act of 2002."

**SECTION 102. TABLE OF CONTENTS.—**The table of contents for this Act is as follows:

101	SECTION 101. SHORT TITLE.
102	SECTION 102. TABLE OF CONTENTS.
103	SECTION 103. PURPOSE AND SCOPE.
104	SECTION 104. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
105	SECTION 105. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
106	SECTION 106. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
107	SECTION 107. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
108	SECTION 108. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
109	SECTION 109. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
110	SECTION 110. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
111	SECTION 111. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
112	SECTION 112. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
113	SECTION 113. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
114	SECTION 114. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
115	SECTION 115. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
116	SECTION 116. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
117	SECTION 117. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
118	SECTION 118. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
119	SECTION 119. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
120	SECTION 120. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
121	SECTION 121. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
122	SECTION 122. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
123	SECTION 123. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
124	SECTION 124. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
125	SECTION 125. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
126	SECTION 126. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
127	SECTION 127. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
128	SECTION 128. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
129	SECTION 129. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
130	SECTION 130. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
131	SECTION 131. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
132	SECTION 132. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
133	SECTION 133. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
134	SECTION 134. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
135	SECTION 135. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
136	SECTION 136. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
137	SECTION 137. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
138	SECTION 138. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
139	SECTION 139. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
140	SECTION 140. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
141	SECTION 141. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
142	SECTION 142. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
143	SECTION 143. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
144	SECTION 144. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
145	SECTION 145. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
146	SECTION 146. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
147	SECTION 147. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
148	SECTION 148. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
149	SECTION 149. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
150	SECTION 150. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
151	SECTION 151. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
152	SECTION 152. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
153	SECTION 153. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
154	SECTION 154. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
155	SECTION 155. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
156	SECTION 156. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
157	SECTION 157. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
158	SECTION 158. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
159	SECTION 159. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
160	SECTION 160. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
161	SECTION 161. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
162	SECTION 162. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
163	SECTION 163. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
164	SECTION 164. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
165	SECTION 165. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
166	SECTION 166. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
167	SECTION 167. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
168	SECTION 168. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
169	SECTION 169. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
170	SECTION 170. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
171	SECTION 171. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
172	SECTION 172. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
173	SECTION 173. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
174	SECTION 174. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
175	SECTION 175. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
176	SECTION 176. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
177	SECTION 177. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
178	SECTION 178. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
179	SECTION 179. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
180	SECTION 180. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
181	SECTION 181. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
182	SECTION 182. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
183	SECTION 183. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
184	SECTION 184. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
185	SECTION 185. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
186	SECTION 186. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
187	SECTION 187. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
188	SECTION 188. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
189	SECTION 189. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
190	SECTION 190. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
191	SECTION 191. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
192	SECTION 192. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
193	SECTION 193. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
194	SECTION 194. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
195	SECTION 195. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
196	SECTION 196. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
197	SECTION 197. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
198	SECTION 198. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
199	SECTION 199. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD
200	SECTION 200. PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD

---

## Handout # 3

- “Long Awaited FFIEC Info Security Exam Handbook Released”
  - Published in the February 2003 edition of Joel Lanz’s ITRISKMGMT Advisor.



---

# 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”.
-

---

## Still not convinced?

- The Information Security Handbook Work Group, one of the two new work groups of the ISC, will continue progress on the Information Security Handbook, a document that addresses information security basics, including a due care standard for negligent liability, for private companies and organizations.

Who are  
these  
people?

---

---

Who would care about a due care  
“security” standard for negligent liability?



- So, what will you do if you actually have an “incident”?



---

WHAT SHOULD AN INCIDENT  
RESPONSE PLAN CONTAIN?

---

---

# Very Hot Topic

- 2003 should be a “break-out” year for this topic
  - Many organizations who do everything else right, are not even close in this area
  - Dust off your business continuity planning and Year 2000 contingency books as they follow a similar process to what’s needed here
-

---

# Think Beyond Your Inner Circle

- Trading Partners
  - Vendors
  - Third-Party Distributors
  - Customers
  - Insurance Carrier
  - Law Enforcement
  - Regulators
-

---

# Preparing for Disasters is a Common Management Challenge

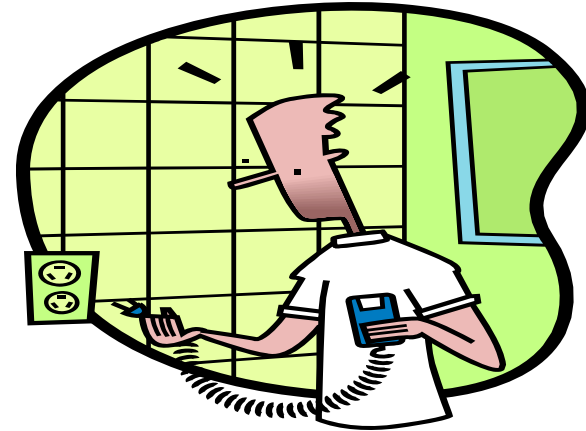
- “Predictable Surprises: The Disasters You Should Have Seen Coming,” Harvard Business Review, Watkins & Bazerman, March 2003.
  - Could the disaster have been avoided?
    - Did the leader recognize the threat?
    - Did the leader prioritize appropriately?
    - Did the leader mobilize effectively?
-

---

# The Typical Team

- IT Security Program Manager (incl. ISO)
  - Legal Department
  - Public Relations
  - HR
  - IT Forensic Expert
  - System Administrators
  - System Owner
  - Technical Specialists
  - Internal Audit
-

# Choose Between Two Strategies



---

# Protect and Forget

- Determine if it is a real incident
  - Terminate the current intrusion
  - Determine how access obtained and what was compromised
  - Restore to pre-incident configuration
  - Secure method of unauthorized access on all systems
  - Document steps taken
  - Develop lessons learned
  - Brief management
-

---

# Apprehend and Prosecute

- Determine if it is a real incident
  - If its is, contact law enforcement
  - Document in detail each action taken
  - Isolate the compromised system from the network
  - Evaluate use of a “honey pot”
  - Identify intruder and document their activity
  - Discover how it happened and secure others
  - Terminate when sufficient evidence has been collected or vital information or systems endangered
  - Document current state for compromised systems
  - Restore compromised systems to pre-incident configuration
  - Secure the “hole” on all other systems
  - Document the cost and time of handling the incident
  - Secure evidence “chain of custody” for future prosecution
  - Develop lessons learned
  - Brief upper management
-

---

# In the Heat of the Battle

- Assess first then act
  - Single intrusion or sophisticated attack
  - Legal and regulatory responsibilities
  - Stop or observe the attack
  - Assessing damage
  - Drain of resources
  - Computer Forensics
-

---

# HOW TO PREPARE FOR IT FORENSICS & FRAUD INVESTIGATIONS?

---

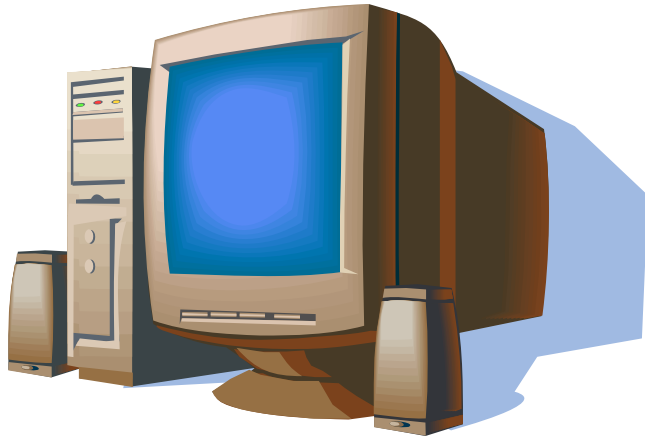
---

## It could be over before it starts....

- Has the right data been captured and maintained for the appropriate period of time?
  - Is there too much pressure to restart and restore system operations?
  - Is there sufficient time to investigate?
-

---

# Some Basic Tools



---

# Don' Just Rush In

- Photograph and label all connectors and plugs to facilitate reconstruction in the forensics lab (and courtroom evidence)
    - For the same cable indicate which side connected to the port and which side connected to the printer
  - Use static free bubble wrap for transport
  - Conduct a disk image backup
    - Remove internal hard disks
    - Place in clean forensic examination machine
    - Make at least 4 copies
    - Place into evidence (packing properly)
    - Restore one copy to identical drive if possible
-

---

# What do you typically do?

- Look for or try to crack passwords
  - Create a map of what's on the disk
  - Search for hidden and deleted files (e.g., Norton Utilities)
  - Use data recovery techniques to recover files
  - Conduct keyword searches with a utility program or primary software
  - Review communication programs for stored numbers
  - Be sensitive to Handheld devices and PC backup tools
-

---

# Warnings

- We've oversimplified for purposes of our presentation
  - Computer Forensics requires special training
    - Fraud Examination
    - Security
    - IT Tools (including vendor)
  - Lots of related certifications – each favoring their sponsors philosophy
    - Vendor
    - Special Interest Group
    - Professional
    - Law Enforcement
  - Know what you need, what you will use it for, and always remember the cost-benefits involved
-

---

# HOW DO YOU MANAGE IT VENDORS & OUTSOURCERS?

---

---

# What Drives Outsourcing?

- Senior Manager's concerns about cost and quality
  - Breakdown in IT Performance
  - Intense vendor pressures
  - Simplified management agenda
  - Financial factors
  - Corporate culture
  - Eliminating an internal irritant
  - Other factors
-

---

# Structuring the Agreement

- Contract Flexibility
  - Standards and Control
  - Areas Outsourced
  - Financial Considerations
  - Cost Savings (if premise for the outsource)
  - Supplier Stability and Quality
  - Management Fit
  - Conversion Management
-

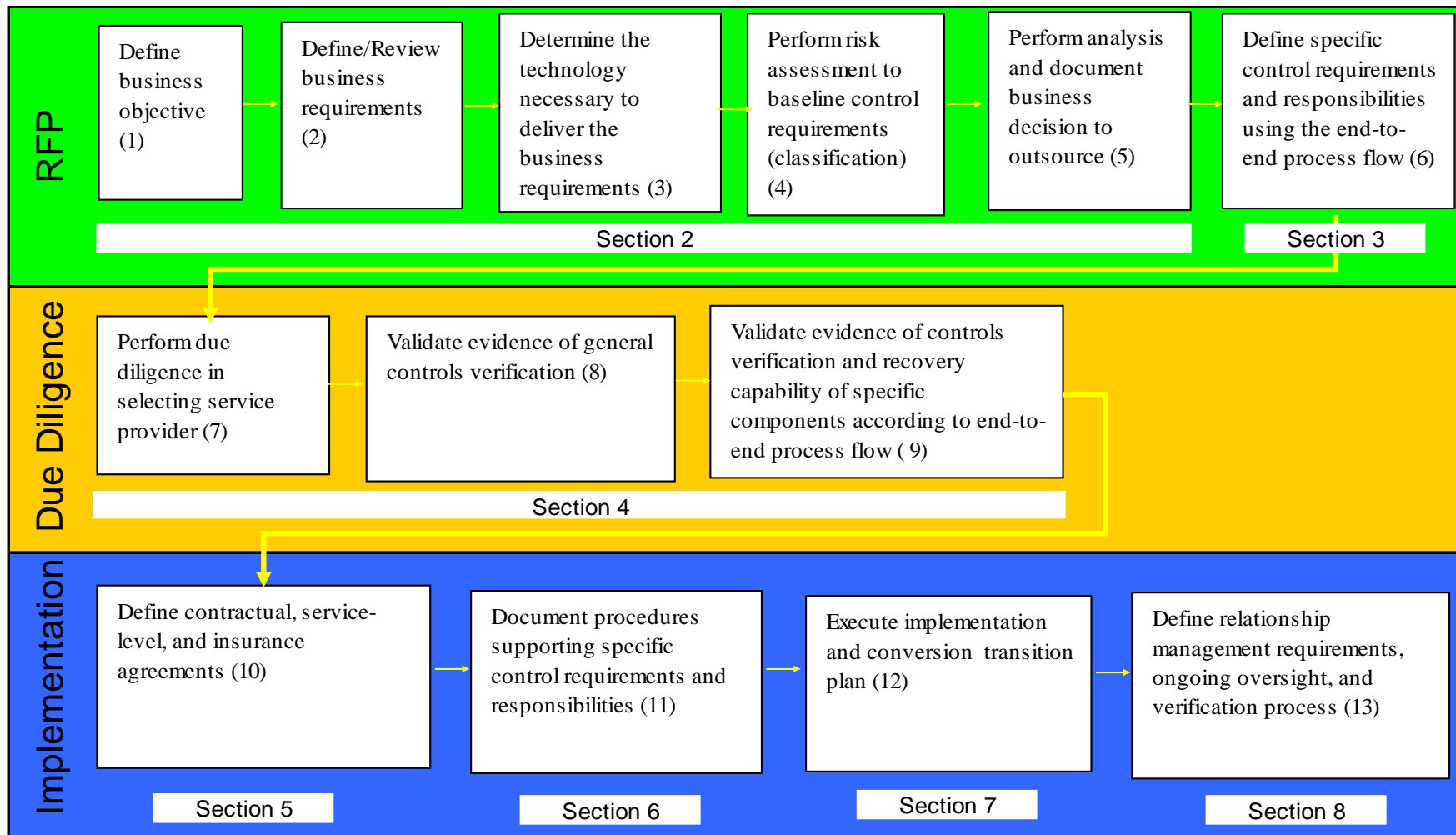
---

# Special Industry Issues

- Confidentiality
  - Privacy
  - Security
  - Regulatory-mandated procedures
  - SAS 70, Trust Services, etc.
  - ISO 17799
  - Cross-Border Issues
-

# BITS FRAMEWORK

(source: BITS Framework: Managing Technology Risk For IT Service Provider Relationships, 10/2001)



---

# Sample BITS Guidance

## ■ DUE DILIGENCE

- Assess audits, security, and performance
- Determine provider's reliance on third parties
- Determine impact on your current partners
- Determine service availability options
- Assess the recovery plan
- Assess testing of the plan
- Determine market reputation

## ■ CONTRACTUAL

- Scope of services
  - Financial soundness and change in business strategy
  - Processing environment
  - Confidentiality
  - Access administration
  - Security
  - Controls verification
  - Change control
  - Records retention
  - Business continuity
  - Regulatory compliance
  - Penalties and exit clause
-

---

# Challenges

- You can't outsource accountability
  - The more you require in the contract – the more you will pay – assuming that an outsourcer/vendor will want to do business with you
  - Understand costs-benefits and don't be afraid to walk away
  - Know what you need and negotiate accordingly
-

---

# HOW SHOULD YOU CONTRACT FOR SECURITY MGT SERVICES?

---

---

# Why is Managed Security Hot?

- “Outsourcing Aids Compliance”, Bank Technology News, Brad Miller, December 2001
  - Pressures faced by small to mid-size enterprises:
    - Increasing regulatory requirements
    - Cyber warfare
    - Patch maintenance
    - Availability of user friendly “hacking” tools
    - Customer privacy expectations
-

---

## Two Primary References You Should Read

- “Outsourcing Managed Security Services,” developed by the Networked Systems Survivability Program at the Software Engineering Institute (leverages BITS Framework).
  - “Guide to Information Technology Security Services – Recommendations of the National Institute of Standards and Technology,” Special Publication 800-35 (Draft)
-

---

# Benefits and Risks

## ■ Benefits

- ❑ Cost
- ❑ Staffing
- ❑ Skills
- ❑ Facilities
- ❑ Objectivity & Independence
- ❑ Security Awareness
- ❑ Prosecution
- ❑ Service Performance
- ❑ Service Security & Technology

## ■ Risks

- ❑ Trust
  - ❑ Dependence
  - ❑ Ownership
  - ❑ Shared Environment
  - ❑ Implementation
  - ❑ Partnership Failure
  - ❑ Hidden Costs & Impacts
  - ❑ Legal & Regulatory Issues
-

---

# Types of Services

- Management
    - Security Program
    - Security Policy
    - Risk Management
    - Security Architecture
    - Certification and Accreditation
    - Security Evaluation of IT Products
  - Operational
    - Contingency Planning
    - Incident Handling
    - Testing
    - Training
  - Technical
    - Firewalls
    - Intrusion Detection
    - Public Key Infrastructure
-

---

# Proposal Evaluation – Business Attributes

- Viability
  - Client Satisfaction
  - Relationships with Other Parties
  - Independent Evaluations
  - Personnel
  - Asset Ownership
  - Contractual Exception, Penalties and Rewards
  - Service Level Agreement
  - Exit Strategy
  - Site Visit
  - Implementation Plan
  - Points of Contact
-

---

# Provider Service Attributes

- Top-level Security Requirements
  - Service Availability
  - Service Architecture
  - Service Hardware and Software
  - Service Scalability
  - Service Levels
  - Reporting Requirements
  - Service Scope
  - Cost
-

---

# Security Practices at Provider and Customer Site

- Security Policies, Procedures, and Regulations
  - Contingency Planning; Operational and Disaster Recovery
  - Physical Security
  - Data Handling
  - Authentication and Authorization
  - Access Control
  - Software Integrity
  - Secure Asset Configuration
  - Backups
  - Monitoring and Auditing
  - Incident Management
-

---

# BITS Annual Review Recommendations

- validation of the ongoing business objectives and the necessity for outsourcing
  - verification that the provider has complied with all negotiated business attributes, service attributes, and security practices and that performance is consistent with expectations
  - a high-level review of all processes
  - an analysis of the financial condition of the provider
  - a review of recent third-party audit reports, such as SAS 70 – Type II results
  - a review of recent security risk evaluation reports, performed by a third party or by the provider
  - a review of recent vulnerability assessments and penetration test results, performed by a third party or by the provider
  - a review of recent client satisfaction survey results, performed by a third party, by the provider or by the client
  - a review of configuration change control records
  - verification that supporting documentation (such as user requests) are in the appropriate files with the appropriate authorizations
  - a review of the provider's service continuity, operational recovery, and disaster recovery test results; verification that the test results meet their objectives
  - results from recently conducted response scenario exercises
  - verification of maintenance on critical service assets such as key applications and security systems (for example, firewalls and intrusion detection systems)
  - verification of key contacts for emergencies or to escalate critical issues
  - a fully documented service description
  - a full inventory and configuration report for servers, routers, any other hardware, as well as software involved in service delivery, along with supporting documentation. The provider indicates which of these the client owns and which are owned by the provider.
  - service system configurations, including any files specific to the service (such as firewall rule sets, IDS signatures)
  - results from “external benchmarking of ‘best-of-breed’ suppliers to reset prices and services levels” or to consider renegotiating these terms
-

---

# 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
-

---

# WHAT IS THE ROLE OF INSURANCE IN MANAGING IT RISK

---

---

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



---

# Insurance Risk Assessment

- Identify critical asset
  - Identify potential undesirable event
  - Assign an impact rating
  - Assign threat category
  - Determine threat rating
  - Identify vulnerability
  - Determine vulnerability rating
  - Determine overall risk
  - Assign risk level criticality
-

---

# What to do about risks identified?

- Avoidance
  - Prevention
  - Reduction
  - Transfer
  - Retention
-

---

If you transfer the risk (insurance) then you'll need to consider the following:

- Advantages of deductibles
  - Tax considerations
  - Selection of the insurer
  - Availability of coverage
  - Cost of coverage
  - Financial solvency
-

---

# TECHIE TOPICS AHEAD



---

# HOW DO YOU MANAGE FIREWALLS AND PUBLIC SERVERS?

---

---

# Leverage The COSO Cube

- **THE CONTROL ENVIRONMENT**, which establishes the foundation for the internal control system by providing fundamental discipline and structure.
  - **RISK ASSESSMENT**, which involves the identification and analysis by management—not the internal auditor—of relevant risks to achieving predetermined objectives.
  - **CONTROL ACTIVITIES**, or the policies, procedures, and practices that ensure management objectives are achieved and risk mitigation strategies are carried out.
  - **INFORMATION AND COMMUNICATION**, which support all other control components by communicating control responsibilities to employees and by providing information in a form and time frame that allows people to carry out their duties.
  - **MONITORING**, which covers the external oversight of internal controls by management or other parties outside the process; or the application of independent methodologies, like customized procedures or standard checklists, by employees within a process.
-

---

# Firewall Deployment Violations

- Did not keep it simple (The KISS principle)
  - Did not use the firewall device as it was intended to be used
  - Did not create defenses in depth – relying on a single firewall rather than multiple for sensitive systems
  - Did not adequately pay attention to internal threats
-

---

# Recommended Firewall Strategies

- Use firewalls to secure internet connections and connections to other networks
  - Examine carefully which firewall and firewall environment is best suited to your needs
  - Create a strong firewall security policy
  - Audit the firewall and its policies at least quarterly
  - Address inherent vulnerabilities in TCP/IP
  - Employ filtering at the firewall for viruses and active content
  - Separate externally accessible systems from private networks
  - Ensure the firewall is well managed
  - Monitor IDS & make adjustments
  - Stay current with internet security information
  - Don't rely exclusively on the firewall
-

---

# Sharing Test Techniques with Your Techie

- Create a test plan
  - Acquire testing tools
  - Test the firewall functions in your test environment
  - Test the firewall functions in your production environment
  - Select and test features related to log files
  - Execute test scenarios
  - Scan for vulnerabilities
  - Design regression testing
-

---

# Why The Web Server Needs Special Attention

- Communicates with untrusted 3<sup>rd</sup> parties
  - Once compromised, increases risk for other network resources
  - Can impact customer's view of the organization and how it does business
  - Can be used to distribute unlawful material to attack other networks resulting in possible legal liability
-

---

# Caring for Baby

- Plan carefully and address the security aspects of deployment of web servers
  - Implement appropriate security management practices and controls to maintain and operate a secure website
  - Deploy, configure and manage web server operating systems and applications to meet the security requirements of the organization
  - Ensure that only appropriate content is published on the website and that the content is adequately protected from unauthorized alteration
  - Active content should be used only after careful consideration of the benefits to be gained and the associated risks
  - Authentication and cryptographic technologies should be used appropriately to protect certain types of sensitive data
  - An ongoing process must be used to maintain the continued security of public web servers
-

---

# WHAT ARE THE CHALLENGES OF ADMINISTERING EMAIL AND PBX?

---

---

# The Need for an Electronics Communication Policy

- Sexual Harassment
  - Race, Age or Other Forms of Discrimination
  - Libel and Slander
  - Insider Trading
  - Trade Secrets
  - Rights of Third Party Access (e.g., govt.)
  - Privacy Rights of Employees
  - Need to Protect System Security and Manage Company Resources
-

---

# Principles of eMail Privacy Protection



INFORMATION AND PRIVACY COMMISSIONER / ONTARIO

- The privacy of e-mail users should be respected and protected.
  - Each organization should create an explicit policy which addresses the privacy of e-mail users.
  - Each organization should make its e-mail policy known to users and inform users of their rights and obligations in regard to the confidentiality of messages on the system.
  - Users should receive proper training in regard to e-mail and the security/privacy issues surrounding its use.
  - E-mail systems should not be used for the purposes of collecting, using and disclosing personal information, without adequate safeguards to protect privacy.
  - Providers of e-mail systems should explore technical means to protect privacy.
  - Organizations should develop appropriate security procedures to protect e-mail messages.
-

---

# eMail Security – the forgotten Risk

- Denial of Service Attacks
  - Disclosure of Sensitive Information on Server on in transit
  - Altering of messages
  - Jump Point to Other Resources (Internal)
  - Attack Other Resources (External)
  - Send Spam (after server is captured)
  - Distribution of Viruses
  - Distribution of Inappropriate, Proprietary or other Sensitive Information
-

---

# What Can You Do?

- Plan carefully and address the security aspects of the deployment of a mail server
  - Implement appropriate security management practices and controls to assure that the mail server is maintained and operated securely
  - Ensure that the mail server operating system and application systems is deployed, configured, and managed to meet the security requirements of the organization
  - Consider implementing cryptography to protect user authentication and mail data
  - Use the network infrastructure to protect the mail servers
  - Continue to maintain the security of mail servers in an ongoing process
-

---

# Why Worry About the PBX?

- Managed “by default”
  - Due to perceived low financial risk, rarely audited by IA or external auditors
  - Risks include:
    - Theft of service
    - Disclosure of information
    - Data modification
    - Unauthorized access
    - Denial of service
    - Traffic analysis
-

---

# PBX Remote Maintenance

## ■ Risks

- ❑ Database upload/download utility
- ❑ Database examine/modify utility
- ❑ Software debugger/update utility (gives unlimited access to PBX and its associated instruments)

## ■ Countermeasures

- ❑ Block remote access unless unattended access required – use local personnel in opening remote maintenance ports
  - ❑ Install two-factor authentication on remote maintenance ports
  - ❑ Keep physically secured
  - ❑ Turn off maintenance when not using
-

---

# PBX Administrative Databases

## ■ Risks

- ❑ Passwords
- ❑ Physical Security
- ❑ Remote Access
- ❑ Software Loading and Update Tampering

## ■ Countermeasures

- ❑ Use hard to break passwords
  - ❑ Leverage error detection codes that are based on strong cryptography
  - ❑ Protect PBX boot disks
  - ❑ Shred printouts when discarded
-

---

# PBX User Features

## ■ Risks

- ❑ Attendant Console (override, forwarding, conferencing)
- ❑ Automatic Call Distribution (can monitor)
- ❑ Account/Authorization Codes (dial in system access)
- ❑ Override
- ❑ Diagnostics
- ❑ Feature Interaction

## ■ Countermeasures

- ❑ Connect attendant console to PBX with different physical connection
  - ❑ Specific line configuration for attendant console.
  - ❑ Consider interaction when adding features
  - ❑ Only activate essential features
-

---

# Computer Telephony

- Voice over IP
  - Browser-based call handling and administration
  - Integration of IP PBX with legacy PBX's and voice systems
  - Integration of wireless and office network systems
  - Virtual Private Networks
-

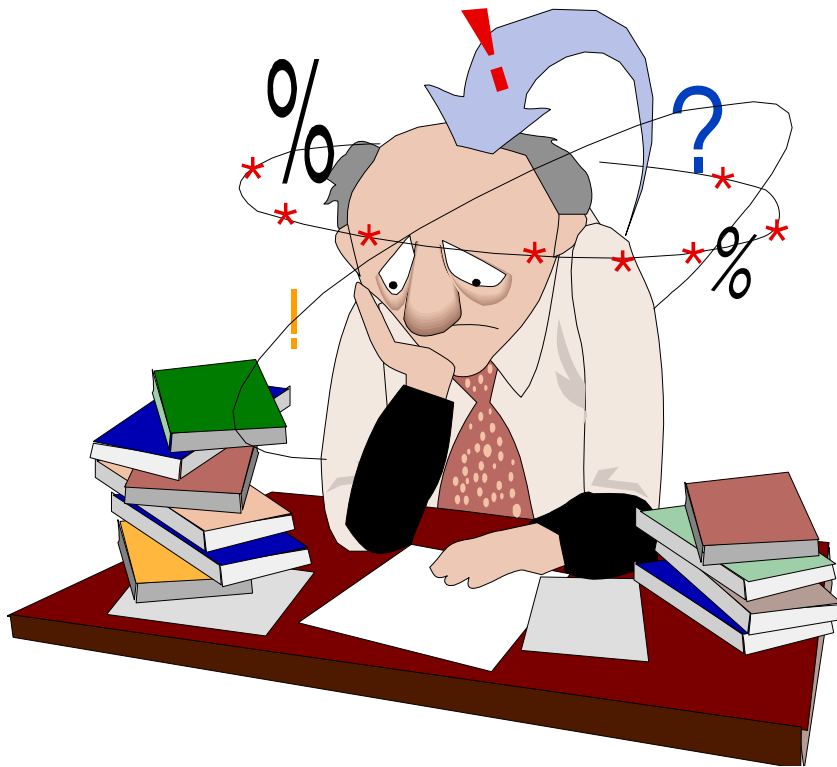
---

WHAT DOES THIS ALL MEAN FOR  
THE INTERNAL AUDITOR?

---

---

# 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

---