

# Understanding an IT Audit

Craig A. Brye, CISA  
Eide Bailly, LLP  
701-476-8319

A stylized silhouette of a mountain range in shades of teal, located at the bottom right of the slide.

# Background

- ◆ Network Administration
- ◆ Network Security
- ◆ Certified Information Systems Auditor (CISA)

# Security Vs. Audit

- ◆ Distinct but complementary
- ◆ More of a focus on internal issues
- ◆ Process oriented
  - Human element
- ◆ A comprehensive and successful security solution
  - Security and Privacy
- ◆ Includes the non-technical aspects of reducing IT risk
- ◆ Treat the symptoms or find a cure

# Current Compliance Programs

- ◆ Sarbanes-Oxley – 404
- ◆ Health Information Portability and Accountability Act (HIPAA)
- ◆ Gramm-Leach-Bliley
  - FDIC, FFIEC
- ◆ FERC/NERC
- ◆ FTC Safeguards Rule

# Reasons to Conduct an Audit

- ◆ The goal of an Information Systems audit is to ascertain the controls in place for all technologies in use and provide an independent opinion on the effectiveness of those controls in regards to containing risk.
- ◆ Regulatory requirements
- ◆ Request from a business partner
- ◆ Marketing
- ◆ Employee Evaluation
- ◆ Pro-active approach to security

# SAS 70

- ◆ Statement on Auditing Standards (SAS) No. 70, *Service Organizations*, is an internationally recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA).
- ◆ A SAS 70 audit or service auditor's examination is widely recognized, because it represents that a service organization has been through an in-depth audit of their control activities, which generally include controls over information technology and related processes.

- ◆ SAS No. 70 allows organizations to disclose their control activities and processes to their customers and their customers' auditors in a uniform reporting format. A SAS 70 examination signifies that a service organization has had its control objectives and control activities examined by an independent accounting and auditing firm.
- ◆ Financial reporting
- ◆ Acceptable format to present to 3<sup>rd</sup> parties
- ◆ Testing of controls

# Defining Scope

- ◆ Most important step
  - Easy to lose focus
- ◆ Select audit programs define scope (e.g. HIPAA)
- ◆ Organization defines “system” (e.g. SAS 70)
  - Can be as broad or as narrow as you deem sufficient

# Vague But True

- ◆ Gramm-Leach-Bliley as an example.
- ◆ Cut and paste the text of the law into MS Word = 270 pages.
- ◆ Look for the section that deals with technology (Sec 501(b))

# 501(b)

- ◆ (b) FINANCIAL INSTITUTIONS SAFEGUARDS- In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards--
  - ◆
  - ◆ (1) to insure the security and confidentiality of customer records and information;
  - ◆
  - ◆ (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and
  - ◆
  - ◆ (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

- ◆ 270 pages of law
- ◆ 3 sentences of IT guidance
  
- ◆ Can't specify technologies
  - Too many options
  - Change too fast
- ◆ Scalability
  - They don't want to write this law again

# The Big Picture

- ◆ IS compliance is not a series of independent events addressing individual technologies that in the end hopefully add up to a complete solution.
  - You're going to run out of fingers to plug the dike.
- ◆ Due to the highly integrated nature of Information Systems, IS compliance must be addressed in a comprehensive manner.
- ◆ Controls should be established that address Information Systems as a whole
  - More thorough
  - Less work
  - Less chance of inadvertent exposure

# The List

- ◆ A comprehensive IS compliance plan should address all of the following that are applicable in a manner that is appropriate for your facility.
- ◆ Due to time constraints and the variety of environments these may be employed, individual items will not be discussed at length.
- ◆ Mainframes/Core Application
- ◆ Local Area Network
- ◆ Wide Area Network
- ◆ Risk Management

- ◆ Workstations
- ◆ Internet Access
- ◆ Physical Security
- ◆ Disaster Recovery planning
- ◆ Documented Policies and Procedures
- ◆ Strategic Planning
- ◆ Training
- ◆ Support
- ◆ Vendors/Contractors
- ◆ System and User Activity Reporting and Review

- ◆ Internal Audit functions
- ◆ Firewalls
- ◆ Telecommunications
- ◆ Remote Access
- ◆ Backups
- ◆ Offsite Storage
- ◆ Inventories
- ◆ Logical Access Schemas
- ◆ Electronic Mail
- ◆ Virus Controls

- ◆ Imaging
  - ◆ Security Breaches
  - ◆ Testing
  - ◆ Internet Services
  - ◆ 3<sup>rd</sup> Party Software
- 
- ◆ Whew!

# Risk Management

- ◆ IS compliance efforts never end. It's an annual cycle of risk assessment and risk mitigation.
- ◆ "the organization's risk assessment should be a written document that develops a thorough process whereby officials identify the location and degree of sensitivity of confidential information, detail specific areas of risk, determine the level of risk, and then determine the best way to mitigate that risk."
- ◆ All IS security planning will either be based on the results or tie back to it

# Information Security Program

- ◆ A security process includes:
  - Identifying risks
  - Forming a strategy to manage those risks
  - Implementing the strategy
  - Provide necessary training
  - Testing the implementation
  - Monitoring the environment to control the risk

# Your Staff

- ◆ At some point in every exit conference I tell the group the same thing.
  - “Your most valuable asset will be an educated end user and your highest element of risk will be an uneducated one.”
- ◆ It is imperative to get your staff involved with IS compliance efforts through education and training.
- ◆ I do not mean:
  - MS Word, Excel, etc training (although still beneficial)
  - Staff need to become technical wizards
- ◆ What is important is that they understand their role and responsibilities regarding the technology in place at your facility.

# Due Diligence

- ◆ If you implement an IS compliance program merely to satisfy the examiners or get a business partner off of your back, you're doing it for the **WRONG** reason.
- ◆ The right reason is to establish a program that helps to reduce the risk to your organization presented by emerging technologies and to help maintain the security and privacy of yours or your customer's information.

# Common Sense

- ◆ Strip away the legalese and the legislative requirements:
  - ◆ 1. Strong Operating Practices
  - ◆ 2. Sound Security Principles
- ◆ Do the Right Thing
  - Dr. Braithwaite – Senior advisor on Health Information Policy, U.S. Department of Health and Human Services (DHHS)

# Mantras

- ◆ Appropriate for your facility
  - Tailored solution
- ◆ Manageable for your staff
  - Skill sets and time involvement
- ◆ Support business goals
  - Should not be counter-productive
- ◆ Creation vs. maintenance
  - Self sustaining program

# End Result

- ◆ Taking a long-term approach, however, you are going to see the benefits
  - Lower risk
  - Less time addressing examiner findings
  - Streamlining the processes dependent on IS
  - Increased security
  - Maximized utilization of technology investment

- Greater awareness to aid in future decision making
  - More informed staff
  - High degree of preparedness for emergencies
- 
- ◆ The economic benefits from IS compliance efforts are derived from maintaining business results and profitability, not from increasing profit.
  
  - ◆ The key to maintaining profitability in a technologically changing environment is how well you maintain control.

# Q & A

