IT Auditing and Computer Forensics

Kevin H. Doar, CISA
Auditor

Discussion Topics

• What is IT Auditing?
• IT Auditor Skillset
• IT Auditing Standards & Frameworks
• IT Controls with Case Examples
• The Direction of IT Audit
• Computer Forensics

What is IT Auditing?
IT Auditing Defined

“The evaluation of Information Systems, practices, and operations to assure the integrity of an entity’s information.”

Source: Information Technology Control and Audit, Auerbach Publications

IT Auditing Roles

- Global Technology Audit Guide (GTAG) #1
  - Assess IT governance
  - Identify and assess risk
  - Assess controls
  - Ensure IT is included in the Audit Plan
  - Ensure IT is considered for each audit

IT Auditor Skillset
I want to be an IT Auditor!

• Basic auditing skills
• Ability to understand both past, present and future technologies
• Educational or work background in computer science or related field

Arguably most important….

Communication skills!!

Source: The Path to IT Audit
https://iaonline.theiia.org/the-path-to-it-audit

IT Auditing Standards & Frameworks
Audit Standards and Guidance

- Institute of Internal Auditors (IIA)
  - Red Book
  - Global Technology Audit Guides (GTAG)
- Government Accountability Office (GAO)
  - Yellow Book
- ISACA

IIA Standards

- 1210.A3 – Internal auditors must have sufficient knowledge of key information risks and controls and available technology-based audit techniques to perform their assigned work. However, not all internal auditors are expected to have the expertise of an internal auditor whose primary responsibility is information technology auditing.

IIA Standards

- 1220.A2 – In exercising due professional care internal auditors must consider the use of technology-based audit and other data analysis techniques.
IIA Standards

- 2110.A2 – The internal audit activity must assess whether the information technology governance of the organization supports the organization’s strategies and objectives.

IIA Guidance

- GTAG publications dedicated to IT
  - “…address timely issues related to information technology (IT) management, risk, control, and security.”
  - 15 volumes #1-17
    - Volume 5 and 6 no longer exist
- GAIT – Guide to the Assessment of IT Risk

GAO Standards

- 3.72: The staff assigned to a GAGAS audit or attestation engagement should collectively possess:
  - d. skills appropriate for the work being performed. For example, skills in:
    - (2) information technology if the work involves review of information systems
GAO Standards

• Internal Control 6.16
  – Information systems controls are often an integral part of an entity’s internal control. The effectiveness of significant internal controls is frequently dependent on the effectiveness of information systems controls. Thus, when obtaining an understanding of internal control significant to the audit objectives, auditors should also determine whether it is necessary to evaluate information systems controls.

GAO Standards

• Information Systems Controls 6.24
  – When information systems controls are determined to be significant to the audit objectives or when the effectiveness of significant controls is dependent on the effectiveness of information systems controls, auditors should then evaluate the design and operating effectiveness of such controls.

ISACA Standards

• Standards for IS Audit and Assurance are mandatory for individuals who hold the Certified Information Systems Auditor (CISA) designation.
ISACA Standards

- The IT Auditor is required to review and assess:
  - **IS Functions Align with Business**
  - Compliance with legal, environmental and information quality
  - Control environment of the Organization
  - Risks that may adversely effect IT

Frameworks

- COBIT
- FISCAM
- FISMA/NIST
- ISO/IEC
- MARS-E
- PCI DSS

COBIT

- Control Objectives for Information and Related Technologies
- ISACA issued
- Developed by the IT Governance Institute
- Focused on aligning IT with business
- Transition period from 4.1 to 5.0
  - 5.0 adds large focus to concept of “enterprise-wide”
FISCAM

- Issued February 2009
- “…presents a methodology for performing information system (IS) control audits of federal and other governmental entities in accordance with professional standards.”
- Primarily on GAGAS audits (yellow book)

NIST

- National Institute of Science and Technology
- Develops minimum IT standards and guidelines for Federal Agencies (800 series)
- Acts in accordance with the Federal Information Security Management Act (FISMA) of 2002

ISO/IEC

- International Organization for Standardization & the International Electrotechnical Commission
- Provides Best Practices
- ISO/IEC 27000 series includes:
  - Information security management system requirements
  - Code of Practice for information security controls
  - Implementation Guidance
  - Measurement Guidance
MARS-E
- Minimum Acceptable Risk Standards for Exchanges
- Issued by the Centers for Medicare & Medicaid Services in response to health exchanges created by the Affordable Care Act
- Attempts to unite federal requirements under NIST, HIPPA (Health Insurance Portability and Accountability Act), the Privacy Act and other federal and state regulations

PCI DSS
- Payment Card Industry Data Security Standards
- Comprehensive requirements for enhancing payment account data security developed by several major credit card companies
- Requirement compliance is based on per year transactions and previous exposures
- Non-compliance can result in fines and penalties

Why do we need IT Audit?
IT Controls with Case Examples
Types of IT Controls

General vs. Application Controls

- Both are needed and required to ensure the Confidentiality, Integrity and Availability (C.I.A. Principle) of data
- Preventive, Detective and Corrective control types
  - Manual, Physical or Logical

General IT Controls

- General IT controls are throughout the IT environment and support numerous activities, but do not link directly to any specific business process or transaction.
  - Access Security
  - Physical Security
  - Separation of Duties

Application Controls

- Application controls relate to a specific computer software application and/or the individual transactions
  - Input Controls
  - Output Controls
  - Processing Controls
Common IT Control Reviews

• Access controls
• User ID authorization and removal
• Disaster recovery
• Device disposal or user recycling
• Computer administrative rights

2013 Statistics

• 63,437 reported security incidents
  – 47,479 were public entities
• 1,367 confirmed data breaches
• 2012 numbers
  – 47,000 security incidents
  – 621 confirmed data breaches

Source: Verizon 2013 Data Breach Investigations Report

2013 Examples

• February – Evernote required 50 million users to change passwords after data breach
• July – Harbor Freight, credit breach in all stores
• August – CNN, New York Times and other media venues Twitter accounts hacked
• September – Vodafone breach, two million customers personal and financial information stolen
• October – Adobe system breach, 38 million accounts affected
**Target**

- December – Target
  - 40 million credit and debit cards
  - 70 million records
  - Installed a top of the line malware detection tool (FireEye) six months before the breach
  - FireEye team identified the attack
    - Target security teams received the report and dismissed it.
    - Option to delete incoming attacks disabled by Target

**South Carolina**

- South Carolina Department of Revenue
  - September 2012
  - 3.8 million social security numbers
  - 3.3 million bank account numbers
  - 700,000 business information/details

**South Carolina**

- How did it happen?
  - Phishing email
    - Using phishing email, stole employee’s credentials
    - Once in, stole more credentials
    - Two days in September, zipped close to 80 gigabytes of data and sent the files to the Internet
  - Lack of controls
    - Very little data encryption (data at rest)
    - No multi-password system (estimated at $12,000)
    - No encryption of laptops or desktops
South Carolina

- Cost
  - $20,000,000
    - Required a loan
    - $12,000,000 of Experian monitoring for hacked persons
    - $5,600,000 for a new encryption system
    - Governor facing re-election consistently attacked for breach

Photo Leaks

- Celebrity iCloud accounts hacked and photos taken and placed on the web.
- No password lock-out on Find My Phone service
  - Brute force attack
  - Once an account is entered, contact info can quickly be stolen

The Direction of IT Audit
Checklist Risk Assessments

• 71A-1 calls for a three year risk assessment
• FISMA requires yearly risk assessments
• Checklist auditing

Move to Continuous Auditing

• State and Federal regulations moving towards continuous auditing
• Audit logs and IT tools for constant monitoring
  – Auditors need access to these tools if in place
  – Auditors need to recommend these tools if not in place

Computer Forensics
Three Elements

- Media Review
- Internet Log Review
- Email Review

Important Statistics

- Salary.com survey revealed the following about Internet use at work:
  - 64 percent of employees visit non-work related websites every day
  - 53 percent admitted to at least two hours a day
- 60% of all online purchasing and 70% of all Internet pornographic traffic occurs from the hours of 9 AM – 5 PM.

Software/Hardware Needed

- Media Review
  - EnCase
  - FTK
  - Can use for Email and Internet reviews
  - White Papers available for hardware requirements
- Internet Review
  - BlueCoat
  - Websense
- Email Review
  - Symantec
Resources and References

• NIST Special Publications (FREE on internet)
• COBIT 5 (FREE to ISACA members)
• GTAG (Free to IIA members)
• Federal, State and Local laws, rules and regulations as applicable to your business

Thank you

Speaker Name: Kevin H. Doar, CISA
Office: Florida Department of Highway Safety and Motor Vehicles