IT Auditing and Automated Tools

Michelle L. Weaver, CISA
Auditor

Discussion Topics
• IT Auditing Defined
• Role of the IT Auditor
• IT Controls
• Auditing Standards
• Resources and References

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
Role of the IT Auditor

- To assess the efficiency and effectiveness of IT
- To assess the availability, integrity, and confidentiality of IT Resources
- To assess the protection/security of IT Resources
- To report IT internal control issues

The role of the IT audit function should be documented within the audit charter. It may include IT audit as well as other audit support functions.

- Due to varying organizational structures the day-to-day role may vary to include:
  - Perform dedicated IT audits of technological subject matter.
  - May include assurance engagements, compliance audits, consulting engagements, and other special projects.
  - Support non-IT auditors with testing IT related subject matter if risk is assessed at a high level.
  - IT audit planning.
  - Due to knowledge and experience, may also be called upon to provide system administration duties, investigative support duties, web support duties, data analytics and other technical assistance.

IT Controls As Defined in the IPPF (RED BOOK)

Controls that support business management and governance as well as provide general and technical controls over information technology infrastructures such as applications, information, infrastructure, and people.
IT Controls As Defined in COBIT

“The policies, procedures, practices and organizational structures, designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected.”

- IT should effectively support the organizations business objectives.

Why Are IT Controls Important?

External Threats

47,000+ reported security incidents, 621 confirmed data disclosures, and at least 44 million compromised records in 2012.

- 92% of incidents were external actors

Source: Verizon 2013 Data Breach Investigations Report
External Threats

Actions Included:
- Tampering (Physical)
- Brute force (Hacking)
- Spyware (Malware)
- Capture stored data (Malware)
- Adminware (Malware)
- RAM Scraper (Malware)
- Backdoor (Malware)
- Phishing (Social)
- Command/Control (Malware, Hacking)
- Export data (Malware)
- Password dumper (Malware)
- Downloader (Malware)
- Stolen creds (Hacking)
- RFI (Hacking)

Assets Targeted Included:
- Laptop/desktop
- File server
- Mail server
- Director server
- Web application
- Database
- ATM
- POS controller
- POS terminal

Source: Verizon 2013 Data Breach Investigations Report

Internal Threats

“Data theft involving programmers, administrators, or executives certainly makes for interesting anecdotes, but is still less common in our overall dataset than incidents driven by employees with little to no technical aptitude or organizational power.”

Source: Verizon 2013 Data Breach Investigations Report

Internal Threats

Still 13% of breaches reported in 2012 were the result of employees misusing technology and associated confidential information.

Source: Verizon 2013 Data Breach Investigations Report
How to control IT Risk?

Types of IT Controls
General vs. Application Controls
- Both are needed/required to ensure the Confidentiality, Integrity and Availability (C.I.A.) of data
- They should consist of Preventive, Detective and Corrective control types
- Can be Manual, Physical or Logical

General IT Controls
- General IT controls are pervasive throughout the IT environment and support numerous activities, but do not link directly to any specific business process or transaction.
General IT Controls

Some General IT control categories include:
• Security Management
• Access Controls
• Configuration Management
• Segregation of Duties
• Business Continuity/Disaster Recovery

Security Management

• Security Management Program
• Periodic Risk Assessments and Validation
• Security Control Policies and Procedures
• Security Awareness Training
• Periodic Testing and Evaluation
• Remediation of Security Weaknesses
• Security Over External Third Parties’ Activities

Access Controls

• Protection of Information System Boundaries
• Identification and Authentication Mechanisms
• Authorization Controls
• Protection of Sensitive System Resources
• Audit & Monitoring Capability Including Incident Handling
• Physical Security Controls
**Configuration Management (CM)**

- CM Policies, Plans & Procedures
- Current Configuration Identification Info
- Proper Authorization, Testing, Approval and Tracking of all Configuration Changes
- Routine Monitoring of the Configuration
- Updating Software on a Timely Basis
- Documentation & Approval of Emergency Changes to the Configuration

**Segregation of Duties**

- Segregation of Incompatible Duties & Responsibilities and Related Policies
- Control of Personnel Activities Through Formal Operating Procedures, Supervision and Review

**Business Continuity / DR**

- Assessment of the Criticality and Sensitivity of Computerized Operations & Identification of Supporting Resources
- Steps Taken to Prevent and Minimize Potential Damage and Interruption
- Comprehensive Contingency Plan
- Periodic Testing and Updating of the Contingency Plan
Application Controls

“Ensure the completeness and accuracy of the records and the validity of the entries made in the transactions and standing data resulting from both manual and automated processing.”

Source: IT Governance Institute, www.itgi.org

Application Controls

• Input Controls
  – Prevents invalid, missing or erroneous data
  – Ensure errors are captured and effectively resolved
• Processing Controls
  – Ensures only authorized and accurate data is stored
• Output Controls
  – Ensures appropriate access and accuracy of data

Input Controls

• Input Authorization
  – Authorized source documents and input files are complete and accurate (e.g. batch totals, sequence checking, etc.)
  – Access Controls (e.g. Segregation of Duties
    – Input data is approved
• Edit Checks (e.g. invalid field lengths or characters, missing data, incorrect data, or erroneous dates)
• Error Processing (e.g. error or warning messages, error reports, etc.)
Processing Controls
- Processing errors are identified, logged and resolved
- Transactions are executed in accordance with predetermined parameters and tolerances
- Transactions are valid and unique (not duplicative)

Output Controls
- Reconciliation
- Distribution of Output is Clearly Defined
- Limited Physical and Logical Access Defined to Authorized Personnel
- Retention

IT Outsourcing
IT Outsourcing
- Includes people, processes, hardware, software, and data.
- Service Level Agreements/Contracts
- Service Organization Control (SOC) Reports
- Service Provider’s Internal Audit Group
- Performance of Independent Testing of the Outside Control Activities

IT Audit Standards

Audit Standards
- Institute of Internal Auditors (IPPF)
- Government Accountability Office (GAO)
- ISACA
IIA Red Book (IPPF) Standards

- 1210.A3 – Internal auditors must have sufficient knowledge of key information technology 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

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

IIA

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

• 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; (3.72)

GO

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 operation effectiveness of such controls. (6.24)

ISACA Standards

• Standards for IS Audit and Assurance are mandatory for individuals who hold the Certified Information Systems Auditor (CISA) designation.
  – Outline minimum level of acceptable performance required to meet the professional responsibilities set out in the ISACA Code of Professional Ethics.
ISACA

The IT Auditor is required to review and assess:

• Whether the IS function aligns with the mission, vision, values, objectives and strategies of the organization.
• Whether the IS function has a clear statement about the performance expected by the business and assess its achievement.
• The effectiveness of IS resource and performance management processes.

ISACA

The IT Auditor is required to review and assess:

• Compliance with legal, environmental and information quality, and fiduciary and security requirements.
• Control environment of the organization
• Risks that may adversely effect IT

ISACA

The IT Auditor is required to:

• Evaluate and monitor IT controls that are an integral part of the internal control environment of the organization.
• Assist management by providing advice regarding the design, implementation, operation and improvement of IT controls.
CAATs or Technology-Based Auditing

Technology-based Audit Techniques

- Any automated audit tool, such as generalized audit software, test data generators, computerized audit programs, specialized audit utilities, and computer-assisted audit techniques (CAATs).
  - Some examples include: MS Excel, MS Access, ACL, IDEA, Automated Work Paper Solutions, etc.

Advantages to Technology Based Auditing Techniques

- Some advantages include:
  - Easier extraction and examination of large volumes of data.
  - Aides in the identification of data anomalies not easily identified via traditional audit sampling (e.g. fraud detection, data analysis, etc.)
  - Customized testing based upon data anomalies.
  - Building of automated scripts aide in continuous auditing/monitoring efforts.
Obstacles to Technology Based Auditing Techniques

- Obtaining reliable data in an effective manner
- Requires experienced, knowledgeable and dedicated staffing resources
- Requires software and hardware that can be expensive

References

Free to IIA Members: GTAG

Global Technology Audit Guide

- Downloads are available for free to IIA members on the IIA website.
- Some available subjects include: IT and Application Controls, Change and Patch Management Controls, Management of IT Auditing, IT Vulnerabilities, IT Outsourcing, ID and Access Management, Business Continuity, IT Audit Planning, Auditing IT Projects & Info. Security & Governance.
Resources and References

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

Thank you

Speaker Name: Michelle L. Weaver, CISA
Office: Department of Health
Email: michelle.weaver@flhealth.gov