IS 369: IT Audit & Controls

Lecture 1

Aron Kondoro

IT Environment

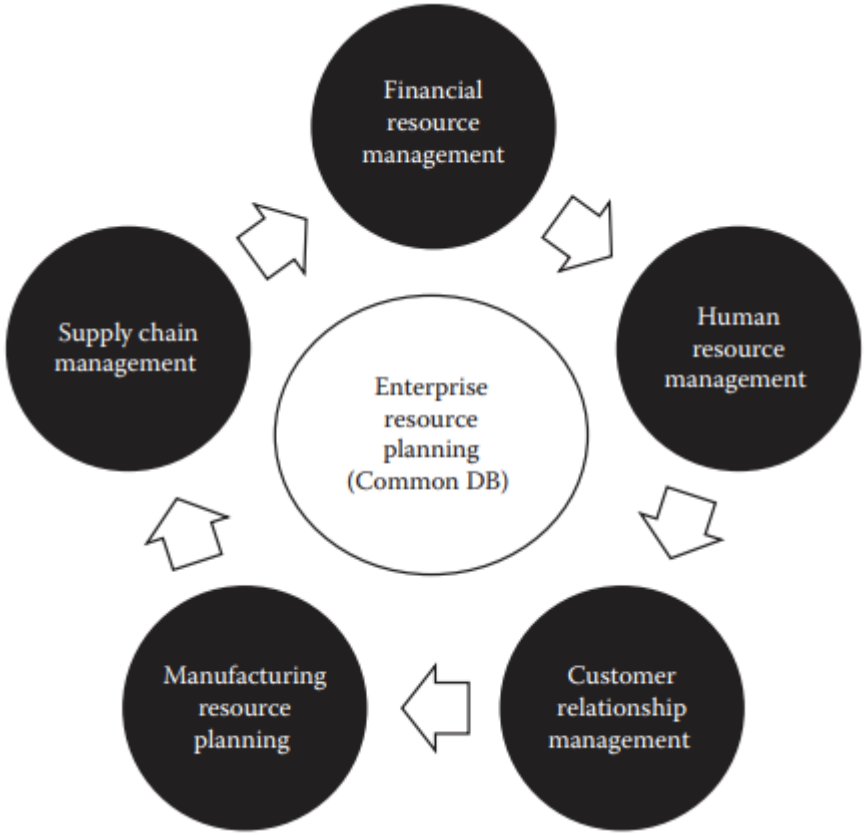
- Recently, Information Technology (IT) has had a significant impact in many areas within public and private organizations
  - Use and processing of information
  - Control process
  - Auditing profession
- Organizations must integrate IT with business strategies to attain overall objectives i.e., profitability, service
- Therefore, need for self-review and self-assurance
- IT Auditors must determine whether the IT controls ensure data protection & align with the overall organization goals

IT Impact

- IT has improved the ability to capture, store, analyze and process huge amounts of business-related data and information
- IT has changed the way in which systems should be controlled
- IT has changed the way auditing is performed
  - Information capture and analysis
  - Control concerns
  - Knowledge required to draw conclusions regarding effectiveness, efficiency, and integrity

Recent Technology Trends

- Enterprise Resource Planning (ERP)
  - Provides standard business functionality in an integrated IT environment
  - Allow multiple functions to access a common database
  - Real time information from modules allow faster generation of financial statements
  - However, ERPs require modifications to fit custom business environments



Recent Technology Trends

- Cloud Computing
  - Organizations use it to perform critical business processes
  - NIST defines cloud computing as “model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be **rapidly provisioned** and released with **minimal management effort** or service provider interaction.”
  - Migrating information to the cloud exposes organizations to new risks e.g., potential unauthorized access to sensitive/critical data (patient data, banking details, personnel records

Recent Technology Trends

- Mobile Device Management (MDM)
  - Management and administration of mobile devices provided to employees as part of their work
  - Bring-your-own-device (BYOD)
  - There is risk to organization's security and employee distraction
  - Need to ensure devices integrate well with the organization and contained corporate information is protected
  - Compliance concerns

Recent Technology Trends

- Internet of Things (IoT)
  - Allows remote assets (things) to interact and communicate among them and with other network systems
  - Provides more accurate understanding and maximizes productivity
- Big Data
  - Large volume of high velocity, complex, and variable data that require advanced techniques and technologies to enable capture, storage, distribution, and analysis of the information
- Challenges
  - Limited access to audit relevant data
  - Scarcity of available and qualified personnel to process and analyze data to integrate into audits

The Auditing Profession

- Computer-related crimes since 1966
- In 1973, Equity Funding Corporation of America (EFCA) declared bankruptcy due to computer-assisted fraud.
  - Company falsified records of its life insurance subsidiary to indicate issuance of new policies. Also falsified other assets such as receivables & market securities
- Lack of IT audit prevented these fictitious assets from being discovered
- Conventional manual techniques were inadequate for audits involving computer applications

The Auditing Profession

- Financial auditing encompasses all activities and responsibilities concerned with rendering of an opinion on the fairness of financial statements
- Scope includes all equipment and procedures used in processing significant data

Internal vs External Audits

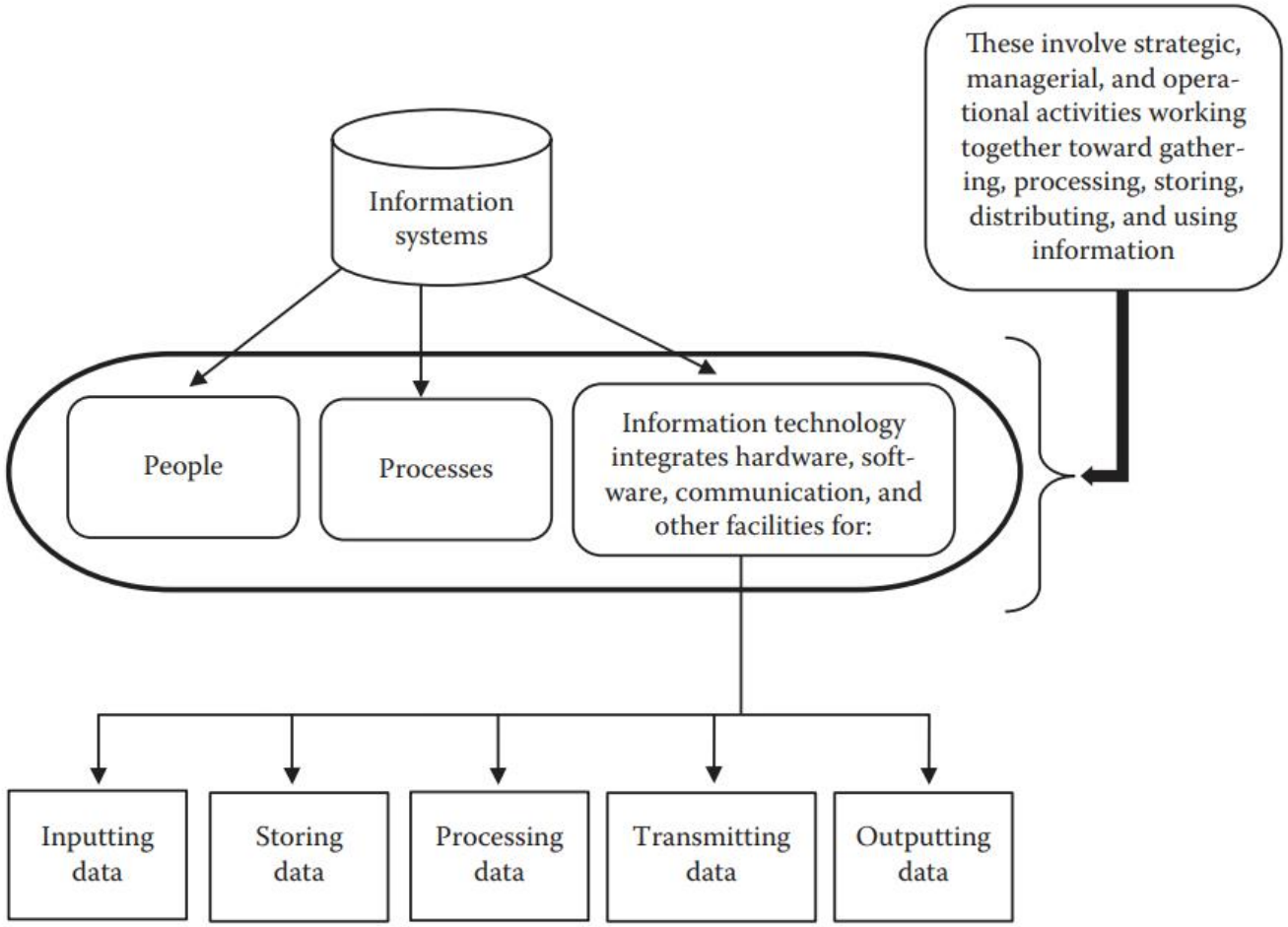
- Aim: To ensure validity and integrity of financial accounting and reporting systems
- Internal Audit
  - Independent, objective assurance and consulting activity designed to add value and improve an organization's operations
  - Assess and enhance risk management, control and governance processes
  - Purpose: assure management-authorized controls are being applied effectively
  - Chief Audit Executive (CAE)
  - All year monitoring and testing of IT activities

Internal vs External Audits

- External Audit
  - Evaluates the reliability and validity of systems controls in all forms
  - Purpose: minimize the amount of substantial auditing or testing of transactions required to render an opinion on the financial statements
  - External auditors: public accounting firms & government
  - National Audit Office of Tanzania (NAOT)
  - Deloitte, Ernst & Young, PricewaterhouseCoopers, and KPMG (“Big Four”)
  - External auditor is responsible for testing the reliability of client IT systems
  - Must have combination of skills and experience to attest all activities and responsibilities associated with rendering an audit opinion on the fairness of the financial statements

IS 369: IT Audit & Controls

IS vs IT



IT Auditing

- IT: hardware, software, communication, and other facilities for managing information
- Audit: Formal inspection and verification to check whether a standard or set of guidelines is being followed, records are accurate, or efficiency and effectiveness targets are being met. (ISACA)

IT Auditing

- *formal, independent, and objective examination of an organization's IT infrastructure to determine whether the activities (e.g., procedures, controls, etc.) involved in gathering, processing, storing, distributing, and using information comply with guidelines, safeguard assets, maintain data integrity, and operate effectively and efficiently to achieve the organization's objectives*

IT Auditing

Information Systems Audit

Information Systems Audit also is the process of deriving assurance on whether the development, implementation, support and maintenance of information systems meets business goals, safeguards information assets and maintains data integrity. The GAG examines the implementation of IT systems and IT controls to ensure that the systems meet the government entities' business needs without compromising security, privacy, cost, integrity of data, availability of data and other critical business elements.

Audit reports issued by CAG on Information Systems Audit

The results of Information Systems Audit are communicated through various reports as explained below:

- **Management letters** which communicates audit findings and recommendations to the management of the audited entities;
- **Annual General Audit Reports** which consolidate key audit findings from management letters of different audited entities and general recommendations addressing to the Government as a whole.

https://www.nao.go.tz/about/information-systems-audit

Why IT Auditing?

- Critical component of enterprise risk management, IT governance, and quality assurance programs and initiatives
- External Audit
  - Publicly traded companies and organizations in many industries are subject to legal and regulatory requirements
  - Organizations seeking various certifications for process or service quality, maturity, or control implementation and effectiveness typically must undergo certification audits by independent auditors
  - provide information that helps organizations manage risk, confirm efficient allocation of IT-related resources, and achieve other IT and business objectives

IS 369: IT Audit & Controls

Why IT Auditing?

- Internal Audit
  - complying with securities exchange rules that companies have an internal audit function
  - evaluating the effectiveness of implemented controls
  - confirming adherence to internal policies, processes, and procedures;
  - checking conformity to IT governance or control frameworks and standards;
  - analysing vulnerabilities and configuration settings to support continuous monitoring;
  - identifying weaknesses and deficiencies as part of initial or ongoing risk management;
  - measuring performance against quality benchmarks or service level agreements;
  - verifying and validating systems engineering or IT project management practices; and
  - self-assessing the organization against standards or criteria that will be used in anticipated external audits.

Why IT Auditing?

- Public Organizations
  - Mandate and Responsibilities of the Controller and Auditor General
  - Required by Section 10 (2) of the Public Audit Act No. 11 of 2008 to satisfy myself that:
    - Accounts have been prepared in accordance with the appropriate accounting standards and legal framework;
    - Reasonable precautions have been taken to safeguard the collection of revenue, receipt, custody, disposal, issue and proper use of public property; and
    - Law, directives and instructions applicable thereto have been duly observed and expenditures of public money have been properly authorized.
  - Evaluate ICT controls to determine whether they are working efficiently and effectively and provide reliable information to users and properly managed to achieve their intended benefits.

IT Auditing

- A growing field with a lot of demand due to IT governance
  - Learning new ways to accomplish tasks faster
  - Organizations need to develop or acquire personnel with the specialized understanding of control objectives and experience in IT operations
  - Big Four have special IT audit groups
  - Assist financial auditors to establish correctness of statements
  - Penetration studies, firewall evaluations, bridges, routers, and gateway configurations

IT Auditing Individuals and Organizations

- Internal auditors i.e., employees, contractors, consultants, or outsourced specialists hired by organizations to carry out internal audits;
- IT auditors working as independent contractors or as employees of professional service firms that provide external or internal IT auditing services;
- Auditing or accounting firms (or the audit or accounting divisions of firms offering a wider range of services);
- Certification organizations authorized to evaluate organizational practices and controls and confer certification to organizations
- Organizations with the authority to oversee the implementation of required controls or enforce regulations e.g., BOT, TCRA
- Inspectors general, audit executives, or equivalent officials charged with the authority to provide independent review of many aspects of the organizations for which they work, including compliance with organizational policies, provision of adequate security, effective allocation of resources, and maintenance of fiduciary responsibility or other standards of care.

IS 369: IT Audit & Controls

Who needs Auditing?

Sector, Industry, or Type	External IT Audit Drivers
Public corporations	SEC rules; Sarbanes–Oxley Act rules on internal controls (§404) [3] and the PCAOB the law created
Financial institutions	Federal Financial Institutions Examination Council IT Examination Handbook, Audit Booklet [11]
Health care organizations	Revisions to Health Insurance Portability and Accountability Act (HIPAA) Security Rule and Privacy Rule in the Health Information Technology for Economic and Clinical Health (HITECH) Act [12]
Nonprofit organizations	Federal and state audits of internal controls for various types of nonprofits, often tied to sources and amount of funding received
Government agencies	Government Auditing Standards (the "Yellow Book") [13]
Federal funding recipients	Single Audit Act of 1984 [14] and OMB Circular A-133, Audits of states, local governments, and nonprofit organizations [15]
Service providers	ISAE 3402: Assurance reports on controls at a service organization [16]

IS 369: IT Audit & Controls

IT Auditing Theory & Methodologies

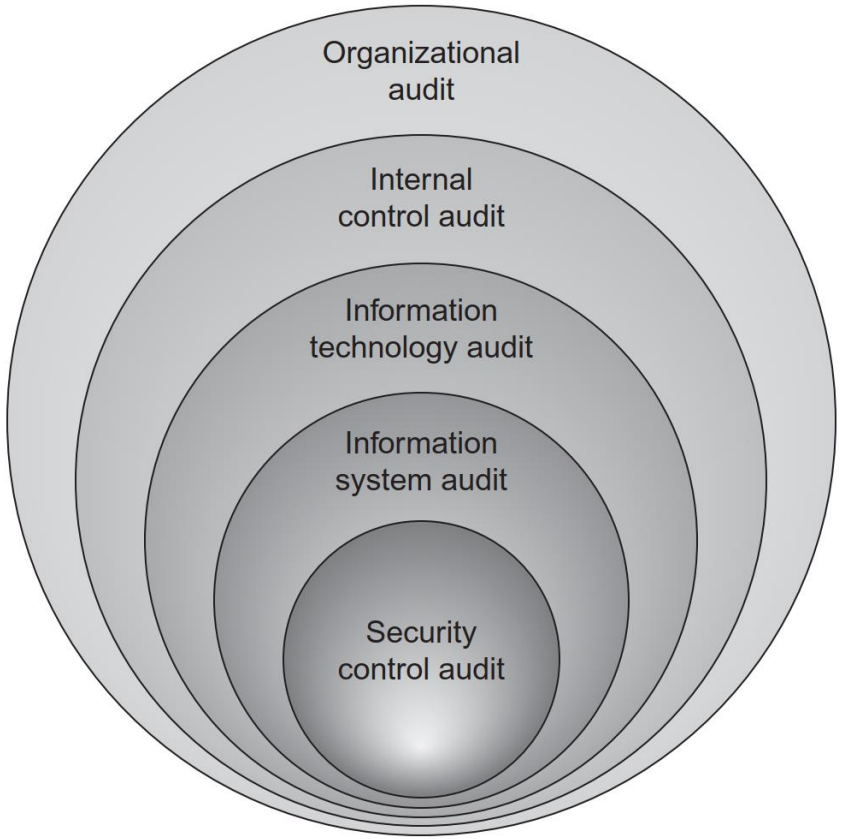
- Fundamental understanding of business
- Traditional Auditing
- IT Management
- Behavioral science
- IT sciences

Types of IT Auditing

- General Computer Controls Audit
  - Examines general IT controls i.e., policies & procedures that support effective functioning of application controls
  - Include controls over IS operations, information security, change control management (CCM)
  - Examples: backups, job monitoring, user account administration, access termination, change request approvals, upgrades, network infrastructure monitoring
- Application Controls Audit
  - Examines processing controls specific to the application i.e., automated controls
  - Concerned with accuracy, completeness, validity, and authorization of data & its management
  - Examples: mathematical accuracy of records, input validation

General Computer Controls vs Application Controls

IT Auditing Scope



IT Auditing Trends

- Due to the importance of computing, the Control Objectives for Information and Related Technology (COBIT) framework was created in 1995 by ISACA
- Increase in reported information theft, computer fraud, decentralization, and other control concerns
- Need to research, develop, publicize, and promote up-to-date, internationally accepted IT control objectives
  - Ensure effective controls are there to maintain data integrity

IS 369: IT Audit & Controls

Principles

- Security: protection against unauthorized access
- Availability: available for operation and use as committed or agreed
- Processing integrity: system processing is complete, accurate, timely, and authorized
- Confidentiality: confidential information is protected as committed or agreed
- Privacy: personal information is collected, used, retained, disclosed in conformity with commitments

Need for IT Audit

- Computers had an impact on auditors' attestation process
- Computers have become a competitive advantage and key resource for businesses hance need for control and auditability
- IT Audit supports auditor's judgement on the quality of information processed by computer systems
- Organizational IT audits, technical IT audits, application IT audits, development IT audits, compliance IT audits

Need for IT Audit

- To assess the increase of sophisticated and "creative" programming
- To support financial statement audits
- To assess the completeness and accuracy of information
- To assess the integrity of information and security of data
- To control the easy access to organization networks from office and remote personal computers
- To support the effective functioning of application controls
- To control and monitor the significant growth of corporate hackers, either internal or external
- To address the rapidly changing technology and the new risks associated with such technology
- To identify controls that can address specific IT risks
- To audit large amounts of data

Role of the IT Auditor

- Provide a statement of assurance whether adequate and reliable internal controls are implemented and are effective and efficient.
- Management: ensure VS Auditor: assure
- Benefits
  - Ensure IT supports business goals
  - Maximize business investment in IT
  - Manage IT-related risks

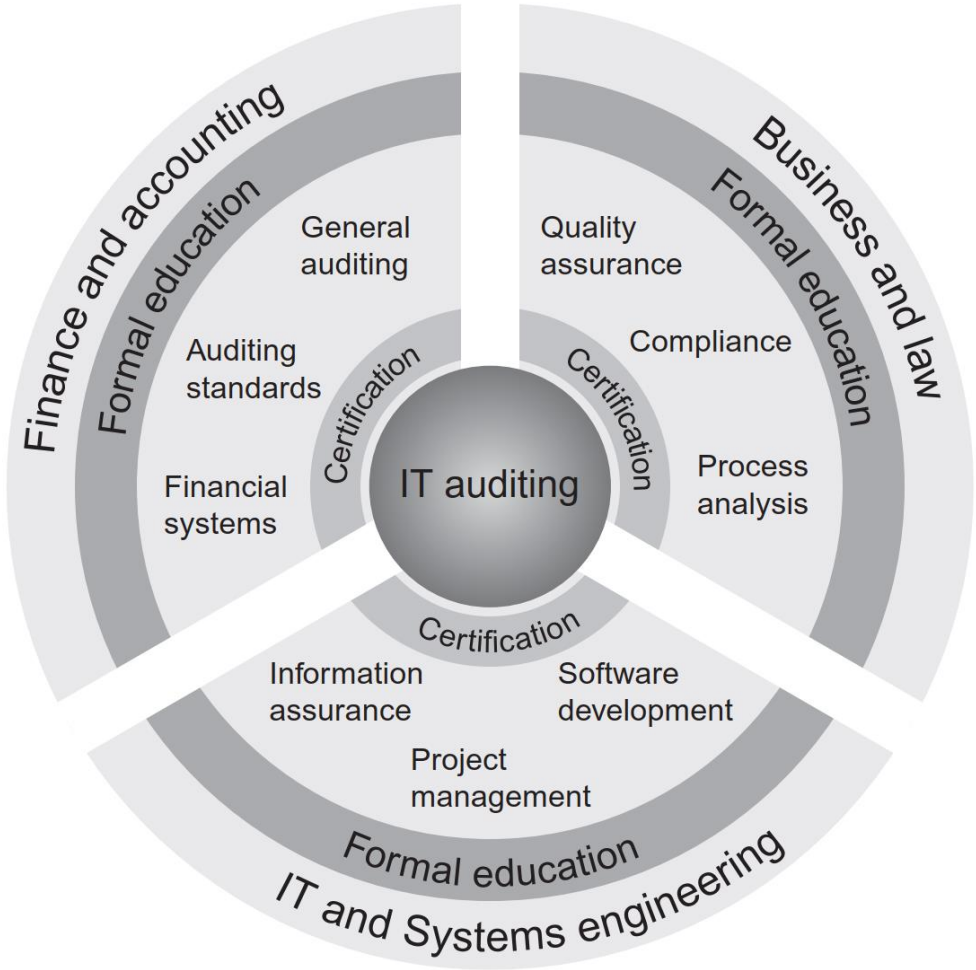
Information Assurance

- The level of confidence and trust that can be placed on the information and service availability
- Goal is to protect users, business units, and enterprises from the negative effects of corruption of information or denial of services
- Scope: local computing environments, boundaries, networks, and supporting infrastructure

IT Audit Profession

- Exposure to way information flows within organization
- Involves people, technology, operations, and systems
- IT auditors interact with managers, users, and technicians
- New profession with
  - Common body of knowledge i.e. core areas of competence (ISACA, CICA etc)
  - Certification i.e. Certified Information Systems Auditor (CISA), also Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified in Risk and Information Systems Control (CRISC)
  - Continuing education
  - Professional associations and ethical standards
  - Educational curriculum

IT Auditor Path



IT Auditor Profile

- Experience
- Understanding of Theory
- Specific industry expertise i.e. banking, telecommunications, insurance etc
- Inter-personal skills
- Presentation skills

Career Opportunities

- Public Accounting Firms
- Private Industry
- Management Consulting Firms
- Government

Further Reading

- Lecture 1 Readings
- Review Questions
- Chapter 1: Otero, Angel R - Information Technology Control and Audit, Fifth Edition
- https://www.nao.go.tz/