Course Outline:

- **Information Technology Environment and IT Audit**
- **IT Environment**
- **The Auditing Profession**
- **IT Auditing and IT Auditing Trends**
- **Role of the IT Auditor**
- **It Audit Responsibilities**

SPECIFIC OBJECTIVES

After this lesson, the student will be able to:

- Discuss how technology is constantly evolving and shaping today's business (IT) environments.
- Discuss the auditing profession and define financial auditing.
- Differentiate between the two types of audit functions that exist today (internal and external).
- Describe current IT auditing trends, and identify the needs to have an IT audit.
- Explain the various roles of the IT auditor.

ACTIVITIES

Instructions upon sending the activity:

a. In one whole sheet of paper, answer the following activities.

Questions:

1. Technology has impacted the business environment in three areas. Summarize those areas.
2. Describe in your own words what IT auditors do.
3. Visit the Websites of four external audit organizations: two private and two government sites. Provide a summary of who they are and their roles, functions, and responsibilities.

Lesson Proper

Introduction to IT Audit and Control

Organizations today are more information-dependent and conscious of the pervasive nature of technology across the business enterprise. The increased connectivity and availability of systems and open environments have proven to be the lifelines of most business entities. Information technology (IT) is now used more extensively in all areas of commerce around the world.

IT Environment

The need for improved control over IT, especially in commerce, has been advanced over the years in earlier and continuing studies by many national and international organizations. Essentially, technology has impacted various significant areas of the business environment, including the use and processing of information, the control process, and the auditing profession.

- Technology has improved the ability to capture, store, analyze, and process tremendous amounts of data and information, expanding the empowerment of the business decision-maker. It has also become a primary enabler of production and service processes. There is a residual effect in that the increased use of technology has resulted in increased budgets, increased successes and failures, and better awareness of the need for **control**.
- Technology has significantly impacted the **control process** around systems. Although control objectives have generally remained constant, except for some that are technology-specific, technology has altered the way in which systems should be controlled. Safeguarding **assets**, as a control objective, remains the same whether it is done manually or is automated. However, the manner by which the control objective is met is certainly impacted.
- Technology has impacted the **auditing profession** in terms of how audits are performed (information capture and analysis, control concerns) and the knowledge required to draw conclusions regarding operational or system effectiveness, efficiency, and reporting **integrity**. Initially, the impact was focused on dealing with a changed processing environment. As the need for **auditors** with specialized technology skills grew, so did the ITauditing profession.

Technology is constantly evolving and finding ways to shape today's IT environment in the organization.

The following sections briefly describe various recent technologies that have and will certainly continue to revolutionize organizations, how business is done, and the dynamics of the workplace.

1. Enterprise Resource Planning (ERP)

According to the June 2016 edition of Apps Run the World, a technology market research company devoted to the applications space, the worldwide market of ERP systems will reach $84.1billion by 2020 versus $82.1 billion in 2015.
ERP is software that provides standard business functionality in an integrated IT environment system (e.g., procurement, inventory, accounting, and human resources [HR]).

ERPs allow multiple functions to access a common database—reducing storage costs and increasing the consistency and accuracy of data from a single source. Additionally, ERPs:
Have standard methods in place for automating processes (i.e., information in the HR system can be used by payroll, help desk, and so on).
Share real-time information from modules (finance, HR, etc.) residing in one common database, hence, financial statements, analyses, and reports are generated faster and more frequently.

Some of the primary ERP suppliers today include SAP, FIS Global, Oracle, Fiserv, Intuit, Inc., Cerner Corporation, Microsoft, Ericsson, Infor, and McKesson.

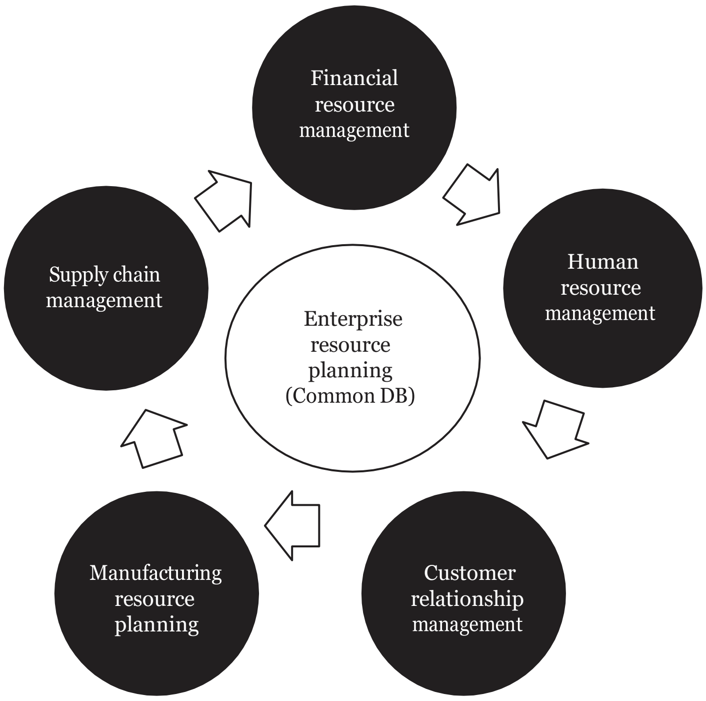

Financial resource management
Human resource management
Customer relationship management
Manufacturing resource planning
Supply chain management
Enterprise resource planning (Common DB)

Exhibit 1.1 Enterprise resource planning modular system.

2. Cloud Computing

Cloud computing continues to have an increasing impact on the IT environment. According to ISACA (formerly known as the Information Systems Audit and Control Association), cloud computing's exponential growth should no longer be considered an emerging technology. Cloud computing has shaped business across the globe, with some organizations utilizing it to perform business-critical processes.

Cloud computing, as defined by PC Magazine, refers to the use of the Internet (versus one's computer's hard drive) to store and access data and programs. In a more formal way, the National Institute of Standards and Technology (NIST) defines cloud computing as a "**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.**" NIST also stresses that availability is significantly promoted by this particular (cloud) model.

The highly flexible services that can be managed in the virtual environment makes cloud computing very attractive for business organizations. Nonetheless, organizations do not yet feel fully comfortable when storing their information and applications on systems residing outside of their on-site premises. Migrating information into a shared infrastructure (such as a cloud environment) exposes organizations' sensitive/critical information to risks of potential unauthorized access and exposure, among others.

3. Mobile Device Management (MDM)

MDM, also known as ***Enterprise Mobility Management***, is a relatively new term, but already shaping the IT environment in organizations. MDM is responsible for managing and administering mobile devices (e.g., smartphones, laptops, tablets, mobile printers, etc.) provided to employees as part of their work responsibilities. Specifically, and according to PC Magazine, MDM ensures these mobile devices:

- integrate well within the organization and are implemented to comply with organization

policies and procedures
- protect corporate information (e.g., emails, corporate documents, etc.) and configuration settings for all mobile devices within the organization

Mobile devices are also used by employees for personal reasons. That is, employees bring their own mobile (personal) device to the organization (also referred to as bring-your-own-device or BYOD) to perform their work. Allowing employees to use organization-provided mobile devices for work and personal reasons has proved to appeal to the average employee. Nevertheless, organizations should monitor and control the tasks performed by employees when using mobile devices, and ensure employees remain focused and productive. It does represent a risk to the organization's security and a distraction to employees when mobile devices are used for personal and work purposes. Additionally, allowing direct access to corporate information always represents an ongoing risk, as well as raises security and compliance concerns to the organization.

Other Technology Systems Impacting the IT Environment

The Internet of Things (IoT) has a potential transformational effect on IT environments, data centers, technology providers, etc. Gartner, Inc. estimates that by the year 2020, IoT will include 26 billion units installed and revenues will exceed $300 billion generated mostly by IoT product and service suppliers.

IoT, as defined by Gartner, Inc., is a system that allows remote assets from "things" (e.g., devices, sensors, objects, etc.) to interact and communicate among them and with other network systems. Assets, for example, communicate information on their actual status, location, and functionality, among others. This information not only provides a more accurate understanding of the assets, but also maximizes their utilization and productivity, resulting in an enhanced decision-making process. The huge volumes of raw data or data sets (also referred to as Big Data) generated as a result of these massive interactions between devices and systems need to be processed and analyzed effectively in order to generate information that is meaningful and useful in the decision-making process.

Other recent technologies listed on the Gartner's 2015 Hype Cycle for Emerging Technologies Report that are currently impacting IT environments include wearables (e.g., smartwatches, etc.), autonomous vehicles, cryptocurrencies, consumer 3D printing, and speech-to-speech translation, among others.

IT Environment as Part of the Organization Strategy

In today's environment, organizations must integrate their IT with business strategies to attain their overall objectives, get the most value out of their information, and capitalize on the technologies available to them. Where IT was formerly viewed as an enabler of an organization's strategy, it is now regarded as an integral part of that strategy to attain profitability and service. At the same time, issues such as IT governance, international information infrastructure, security, privacy and control of public and organization information have driven the need for self-review and self-assurance.

For the IT manager, the words "**audit**" and "**auditor**" send chills up and down the spine. Yes, the auditor or the audit has been considered an evil that has to be dealt with by all managers. In the IT field, auditors in the past had to be trained or provided orientation in system concepts and operations to evaluate IT practices and applications. IT managers cringe at the auditor's ability to effectively and efficiently evaluate the complexities and grasp the issues. Nowadays, IT auditors are expected to be well aware of the organization's IT infrastructure, policies, and operations before embarking in their reviews and examinations. More importantly, IT auditors must be capable of determining whether the **IT controls** in place by the organization ensure data protection and adequately align with the overall organization goals.

Professional associations and organizations such as ISACA, the **American Institute of**

Certified Public Accountants (AICPA), the Canadian Institute of Chartered Accountants (CICA), Institute of Internal Auditors (IIA), Association of Certified Fraud Examiners (ACFE), and others have issued guidance, instructions, and supported studies and research in audit areas.

The Auditing Profession

Computers have been in use commercially since 1952. Computer-related crimes were reported as early as 1966. However, it was not until 1973, when the significant problems at Equity Funding Corporation of America (EFCA) surfaced, that the auditing profession looked seriously at the lack of controls in computer information systems (IS). In 2002, almost 30 years later, another major **fraud** resulted from corporate and accounting scandals (Enron and WorldCom), which brought **skepticism** and downfall to the financial markets. This time, neither the major accounting firms nor the security- and exchange-regulated businesses in major exchanges were able to avoid the public outrage, lack of investor confidence, and increased government regulation that befell the U.S. economy.

When EFCA declared bankruptcy in 1973, the minimum direct impact and losses from illegal activity were reported to be as much as $200 million. Further estimates from this major financial fraud escalated to as much as $2 billion, with indirect costs such as legal fees and depreciation included. These losses were the result of a “computer-assisted fraud” in which a corporation falsified the records of its life insurance **subsidiary** to indicate the issuance of new policies.

As the computer was used to manipulate files as a means of covering the fraud, the accounting profession realized that conventional, manual techniques might not be adequate for audit engagements involving computer application. In 1973, the AICPA (major national professional organization of certified public accountants), in response to the events at EFCA, appointed a special committee to study whether the auditingstandards of the day were adequate in such situations.

The committee was requested to evaluatespecific procedures to be used and the general standards to be approved. In 1975, the committee issued its **findings**. Even though the special committee found that auditing standards were adequate and that no major changes were called for in the procedures used by auditors, there were several observations and recommendations issued related to the use of computer programs designed to assist the **examination** of financial statements.

FINANCIAL AUDITING

Financial auditing encompasses all activities and responsibilities concerned with the rendering of an opinion on the fairness of financial statements. The basic rules governing audit opinions indicate clearly that the scope of an audit covers all equipment and procedures used in processing significant data.

Financial auditing, as carried out today by the independent auditor, was spurred by legislation in 1933 and 1934 that created the SEC. This legislation mandated that “companies whose securities were sold publicly be audited annually by a Certified Public Accountant (CPA)”. CPAs, then, were charged with attesting to the fairness of financial statements issued by companies that reported to the SEC to further define the importance of **internal control** in the **attestation engagement**.

Within the CPA profession in the United States, two groups of principles and standards have been developed that affect the preparation of financial statements by publicly held companies and the procedures for their audit examination by CPA firms: **Generally Accepted Accounting Principles (GAAP)** and **Generally Accepted Auditing Standards (GAAS)**.

GAAP establishes consistent guidelines for financial reporting by corporate managers. As part of the reporting requirement, standards are also established for the maintenance of financial records on which periodic statements are based. An auditor, rendering an opinion indicating that financial statements are stated fairly, stipulates that the financial statements conform to GAAP. These accounting principles have been formulated and revised periodically by private-sector organizations established for this purpose. The present governing body is the **Financial Accounting Standards Board (FASB)**. Implementation of GAAP is the responsibility of the management of the reporting entity.

GAAS, the second group of standards, was adopted in 1949 by the AICPA for audits. These audit standards cover three categories:

- *General Standards* relate to professional and technical competence, **independence**, and due professional care.
- *Standards of Fieldwork* encompass planning, evaluation of internal control, sufficiency of evidential matter, or documentary evidence upon which findings are based.
- *Standards of Reporting* stipulate compliance with all accepted auditing standards, consis- tency with the preceding account period, adequacy of disclosure, and, in the event that anopinion cannot be reached, the requirement to state the assertion explicitly.

GAAS provides broad guidelines, but not specific guidance. The profession has supplemented the standards by issuing statements of authoritative pronouncements on auditing. The most comprehensive of these is the SAS series. SAS publications provide procedural guidance relating to many aspects of auditing. In 1985, the AICPA released a codification of the SAS No. 1–49. Today, the number of statements exceeds 120.

A third group of standards, called the **International Financial Reporting Standards (IFRS)**, has been recently created by the **International Accounting Standards Board (IASB)*** to respond to the increasing global business environment and address the need to compare financial statements prepared in different countries. The AICPA defines IFRS as the "set of accounting standards developed by the IASB that is becoming the global standard for the preparation of public company financial statements."

Internal versus External Audit Functions

There are two types of audit functions that exist today. They have very important roles in assuring the **validity** and integrity of financial accounting and reporting systems. They are the internal and external audit functions.

✓ Internal Audit Function

The IIA defines internal auditing (IA) as "an independent, objective **assurance** and consulting activity designed to add value and improve an organization's operations." IA brings organizationsa systematic and disciplined approach to assess and enhance their **risk management**, control, and governance processes, as well as to accomplish their goals and objectives.

IA departments are typically led by a **Chief Audit Executive (CAE)**, who directly reportsto the **Audit Committee** of the **Board of Directors**. The CAE also reports to the organiza- tion's **Chief Executive Officer (CEO)**. The primary purpose of the IA function is to assure that management-authorized controls are being applied effectively. The IA function, although not mandatory, exists in most private enterprise or corporate entities, and in government (such as federal, state, county, and city governments). The mission, character, and strength of an IA function vary widely within the style of top executives and traditions of companies and organizations. IT audits is one of the areas of support for IA.

The IA group, if appropriately staffed with the resources, performs all year long monitoring and testing of IT activities within the control of the organization. Of particular concern to private corporations is the processing of data and the generation of information of financial relevance or **materiality**.

Given management's large part to play in the effectiveness of an IA function, their concern with the **reliability** and integrity of computer-generated information from which decisions are made is critical. In organizations where management shows and demonstrates concern about internal controls, the role of the IA grows in stature. As the IA function matures through experience, training, and career development, the external audit function and the public can rely on the quality of the internal auditor's work. With a good, continuously improving IA management and staff, the Audit Committee of the Board of Directors is not hesitant to assign additional reviews, consultation, and testing responsibilities to the internal auditor. These responsibilities are oftenbroader in scope than those of the external auditor.

✓ External Audit Function

The external audit function evaluates the reliability and the validity of systems controls in all forms. The principal objective in such evaluation is to minimize the amount of substantial auditing or testing of transactions required to render an opinion on the financial statements.

External auditors are provided by public accounting firms and also exist in government as well. For example, the Government Accountability Office (GAO) is considered an external reviewer because it can examine the work of both federal and private organizations where federal funds are provided. The Watchdogs of Congressional Spending provide a service to the taxpayer in report- ing directly to Congress on issues of mismanagement and poor controls. Interestingly, in foreign countries, an Office of the Inspector General or Auditor General's Office within that country prepares similar functions. Also, the GAO has been a strong supporter of the International Audit Organization, which provides government audit training and guidance to its international audit members representing governments worldwide.

From a public accounting firm standpoint, firms such as Deloitte, Ernst & Young, PricewaterhouseCoopers, and KPMG (altogether referred to as the "Big Four") provide these types of external audit services worldwide. The external auditor is responsible for testing the reliability of client IT systems and should have a special combination of skills and experience. Such an auditor must be thoroughly familiar with the audit **attest** function. The attest function encompasses all activities and responsibilities associated with the rending of an audit opinion on the fairness of the financial statements. Besides the accounting and auditing skills involved in performing the attest function, these external auditors also must have substantial IT audit experience. SOX now governs their role and limits of services that can be offered beyond audit.

What Is IT Auditing?

Before defining what IT auditing is, let us explain the difference between IS and IT. An IS, represented by three components (i.e., people, process, and IT), is the combination of strategic, managerial, and operational activities involved in managing information. The IT component of an IS involves the hardware, software, communication, and other facilities necessary to manage (i.e., input, store, process, transmit, and output) such information. Refer to Exhibit 1.2.

The term audit, according to ISACA, refers to the 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. In combining both definitions above, IT auditing can be defined as the *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 provides **reasonable assurance** (never absolute) that the information generated by applications within the organization is accurate, complete, and supports effective decision making consistent with the nature and scope of the engagement previously agreed.

IT auditing is needed to evaluate the adequacy of application systems to meet processing needs, evaluate the adequacy of internal controls, and ensure that assets controlled by those systems are adequately safeguarded. As for the IT auditors of today, their advanced knowledge and skills will progress in two ways. One direction is continued growth and skill in this profession, leading the way in computer audit research and development and progressing up the external and internal audit career paths. The other direction involves capitalizing on a thorough knowledge of organizational systems and moving into more responsible career areas in general management. Today, even in these economic times, the demand for qualified IT auditors exceeds the supply. IT governance has created vast opportunities for the IT auditor.

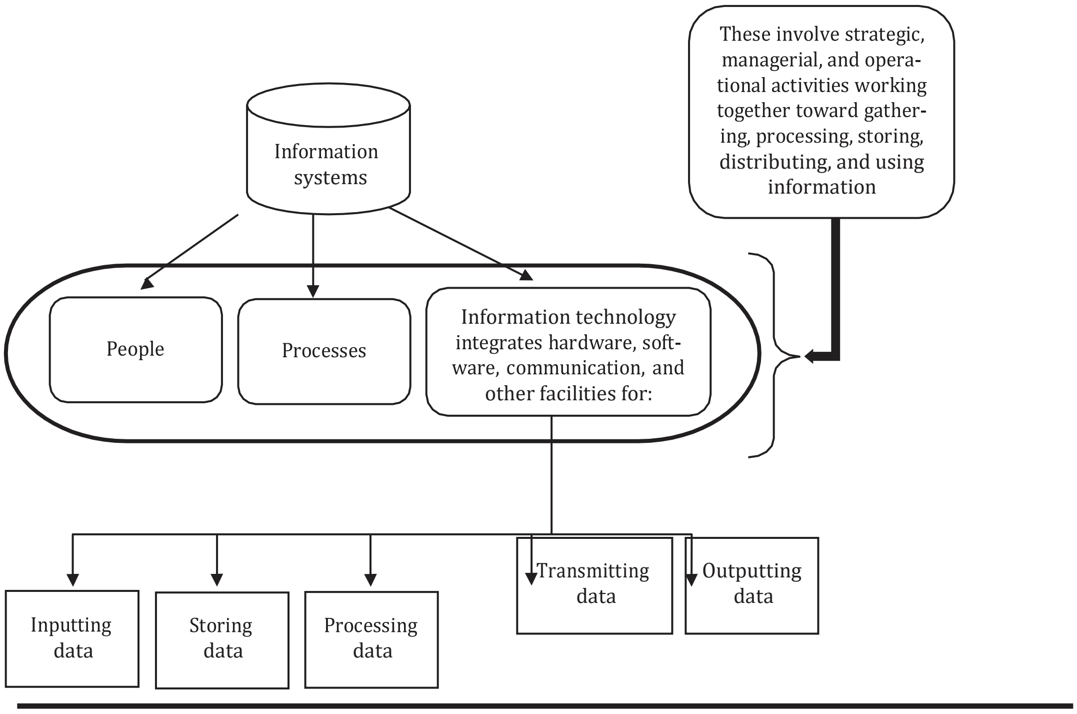

These involve strategic, managerial, and operational activities working together toward gathering, processing, storing, distributing, and using information
Information systems
People
Processes
Information technology integrates hardware, software, communication, and other facilities for:
Inputting data
Storing data
Processing data
Transmitting data
Outputting data

Exhibit 1.2 Information systems versus information technology.

Learning new ways of auditing is always a priority of internal and external IT auditors. Most auditors want tools or audit methodologies that will aid them in accomplishing their task faster and easier. Almost every large organization or company has some sort of IT audit function or shop that involves an internal audit department. Today, the "Big Four" firms have designated special groups that specialize in the IT audit field. They all have staff that perform these external IT audits. Most of these IT auditors assist the financial auditors in establishing the correctness of financial statements for the companies in which they audit. Others focus on special projects suchas Internet security dealing with penetration studies, firewall evaluations, bridges, routers, and gateway configurations, among others.

There are two broad groupings of IT audits, both of which are essential to ensure the contin ued proper operation of IS. These are as follows:

- *General Computer Controls Audit.* It examines IT general controls ("general controls" or "ITGCs"), including policies and procedures, that relate to many applications and supports the effective functioning of application controls. General controls cover the IT infrastructure and support services, including all systems and applications. General controls commonly include controls over (1) IS operations; (2) information security (ISec); and (3) change control management (CCM) (i.e., system software acquisition, change and maintenance, program change, and application system acquisition, development, and mainte nance). Examples of general controls within IS operations address activities such as data backups and offsite storage, job monitoring and tracking of exceptions to completion, and access to the job scheduler, among others. Examples of general controls within ISec address activities such as access requests and user account administration, access terminations, and physical security. Examples of general controls within CCM may include change request approvals; application and database upgrades; and network infrastructure monitoring, security, and change management.

- *Application Controls Audit*. It examines processing controls specific to the application. Application controls may also be referred to as "automated controls." They are concerned with the accuracy, completeness, validity, and authorization of the data captured, entered, processed, stored, transmitted, and reported. Examples of application controls include checking the mathematical accuracy of records, validating data input, and performing numerical sequence checks, among others. Application controls are likely to be effective when general controls are effective.

Refer to Exhibit 1.3 for an illustration of general and application controls, and how they should be in place in order to mitigate risks and safeguard applications. Notice in the exhibit that the application system is constantly surrounded by risks. Risks are represented in the exhibit by explosion symbols. These risks could be in the form of unauthorized access, loss or theft of equipment and information, system shutdown, etc. The general controls, shown in the hexagon symbols, also surround the application and provide a "protective shield" against the risks. Lastly, there are the application or automated controls which reside inside the application and provide first-hand protection over the input, processing, and output of the information.

IT Auditing Trends

Computing has become indispensable to the activities of organizations worldwide. The Control Objectives for Information and Related Technology (COBIT) Framework was created in 1995 by ISACA. COBIT, now on its fifth edition, emphasizes this point and substantiates the need to research, develop, publicize, and promote up-to-date, internationally accepted IT control objectives. In earlier documents such as the 1993 discussion paper "Minimum Skill Levels in Information Technology for Professional Accountants" and their 1992 final report "The Impact of Information Technology on the Accountancy Profession," the International Federation of Accountants (IFAC) acknowledges the need for better university-level education to address growing IT control concerns and issues.

Reports of information theft, computer fraud, information abuse, and other related control concerns are being heard more frequently around the world. Organizations are more information-conscious, people are scattered due to decentralization, and computers are used more extensively in all areas of commerce. Owing to the rapid diffusion of computer technologies and the ease of information accessibility, knowledgeable and well-trained IT auditors are needed to ensure that more effective controls are put in place to maintain data integrity and manage access to information. The need for better controls over IT has been echoed in the past by prior studies such as the AICPA Committee of Sponsoring Organizations of the Treadway Commission (COSO);

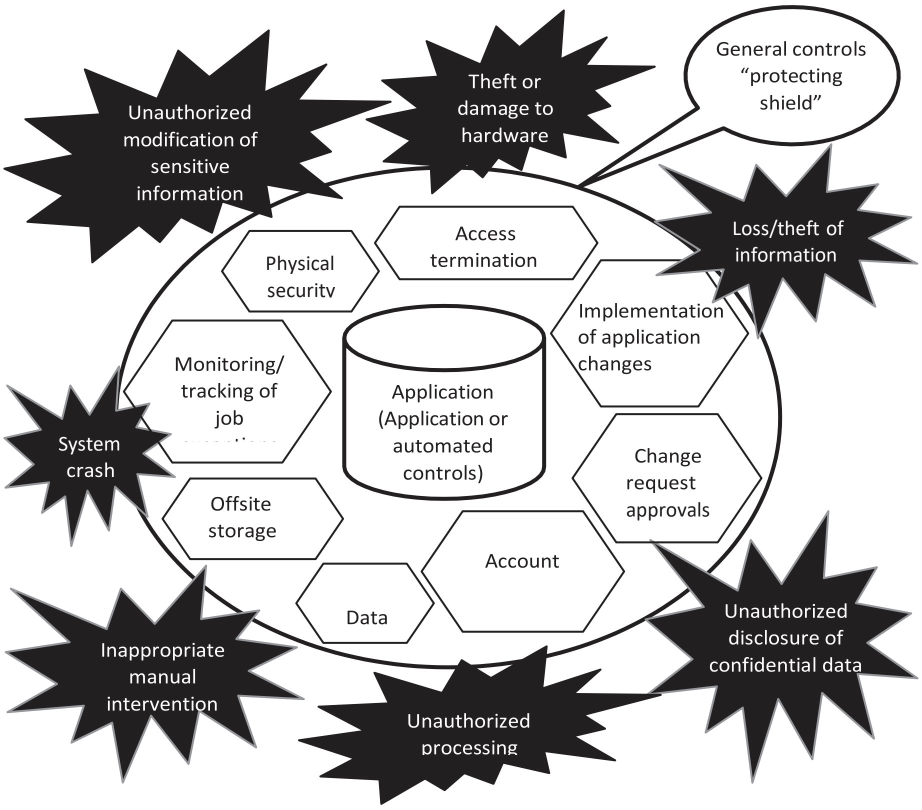

Unauthorized modification of sensitive information
Theft or damage to hardware
General controls "protecting shield"
Loss/theft of information
Physical security
Access termination
Implementation of application changes
Monitoring/ tracking of job
System crash
Application (Application or automated controls)
Change request approvals
Offsite storage
Account
Data
Unauthorized disclosure of confidential data
Inappropriate manual intervention
Unauthorized processing

Exhibit 1.3 Relationship between general computer controls and application controls.

International Organization for Standardization (ISO) 17799 and 27000; the IIA Systems Auditability and Control Report; Guidelines for the Security of IS by the OECD; the U.S. President's Council onIntegrity and Efficiency in Computer Audit Training curriculum; and the United States' National Strategy for Securing Cyberspace released in 2002; among others.

The AICPA's Assurance Services Executive Committee (ASEC) is responsible for updating and maintaining the Trust Services Principles and Criteria (TSPC) and creating a framework of principles and criteria to provide assurance on the integrity of information. TSPC presents criteria for use by practitioners when providing professional attestation or **advisory** services to assess controlsrelevant to the following principles:

- *Security*: The system is protected against unauthorized access (both physical and logical).
- *Availability*: The system is available for operation and use as committed or agreed.
- *Processing integrity*: System processing is complete, accurate, timely, and authorized.
- *Confidentiality*: Information designated as confidential is protected as committed or agreed.
- *Privacy*: Personal information is collected, used, retained, disclosed, and destroyed in conformity with the commitments in the entity's privacy notice and with criteria set forth ingenerally accepted privacy principles issued by the AICPA and CICA.

Ever since the ISACA was formed there has been a growing demand for well-trained and skilled IT audit professionals. The publication *The EDP Auditors Association: The First Twenty-Five Years* documents the early struggles of the association and the evolution of IT audit practices in this field.

The area of information assurance has also grown and evolved. The United States in its passage of the Cyber Security Research and Development Act has pledged almost a billion dollars for the development of curriculum, research, and skills for future professionals needed in this field.

Need for IT Audit

Initially, IT auditing (formerly called electronic data processing [EDP], computer information systems [CIS], and IS auditing) evolved as an extension of traditional auditing. At that time, the need for an IT audit came from several directions:

- Auditors realized that computers had impacted their ability to perform the attestation function.
- Corporate and information processing management recognized that computers were key resources for competing in the business environment and similar to other valuable business resource within the organization, and therefore, the need for control and auditability were critical.
- Professional associations and organizations, and government entities recognized the need for IT control and auditability.

The early components of IT auditing were drawn from several areas. First, traditional auditing contributes knowledge of internal control practices and the overall control philosophy. Another contributor was IS management, which provides methodologies necessary to achieve successful design and implementation of systems. The field of behavioral science provided such questions and analysis to when and why IS are likely to fail because of people problems. Finally, the field of computer science contributes knowledge about control concepts, discipline, theory, and the formal models that underlie hardware and software design as a basis for maintaining data validity, reliability, and integrity.

IT auditing became an integral part of the audit function because it supports the auditor's judgment on the quality of the information processed by computer systems. Auditors with IT audit skills were viewed as the technological resource for the audit staff. The audit staff often looked to them for technical assistance. The IT auditor's role evolved to provide assurance that adequate and appropriate controls are in place. Of course, the responsibility for ensuring that adequate internal controls are in place rests with management. The audit's primary role, except in areas of management advisory services, is to provide a statement of assurance as to whether adequate and reliable internal controls are in place and are operating in an efficient and effective manner. Management's role is to ensure and the auditors' role is to assure.

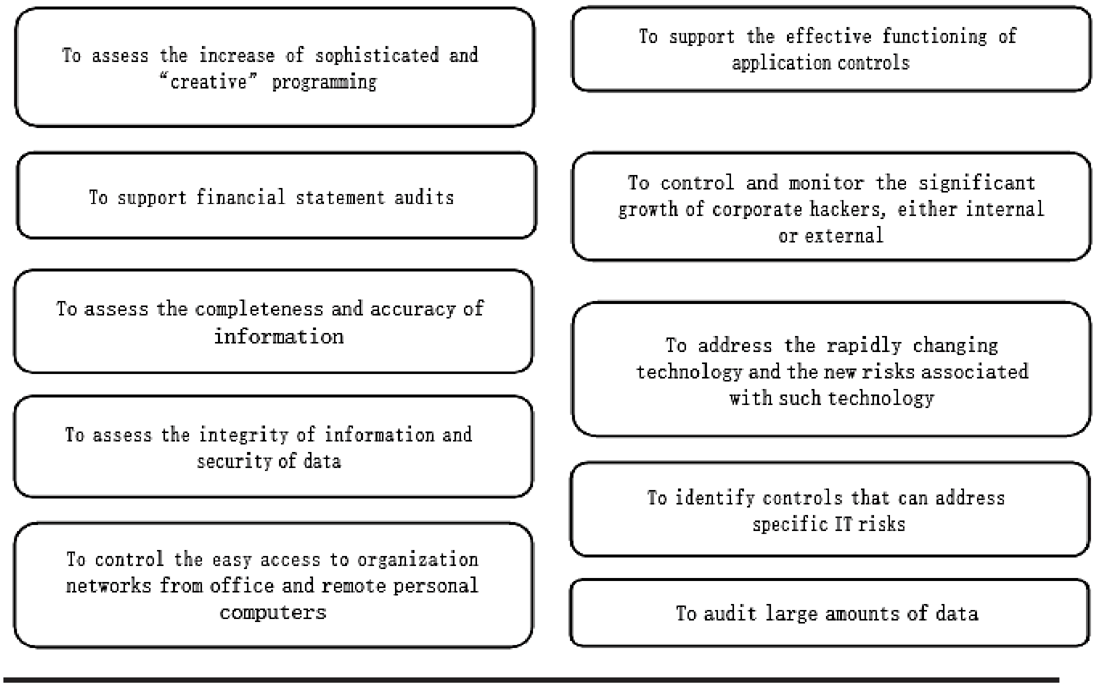
There are several types of needs within IT auditing, including organizational IT audits (management control over IT), technical IT audits (infrastructure, data centers, data communication), and application IT audits (business/financial/operational). There are also development/implementation IT audits (specification/requirements, design, development, and post-implementation phases), and compliance IT audits involving national or international standards.

When auditing IT, the breadth and depth of knowledge required are extensive. For instance, auditing IT involves:

- Application of risk-oriented audit approaches
- Use of computer-assisted audit tools and techniques
- Application of standards (national or international) such as the ISO* to improve and implement quality systems in software development and meet IT security standards
- Understanding of business roles and expectations in the auditing of systems under development as well as the purchase of software packaging and project management
- **Assessment** of information security, confidentiality, privacy, and availability issues which can put the organization at risk
- Examination and verification of the organization's compliance with any IT-related legal issues that may jeopardize or place the organization at risk
- Evaluation of complex systems development life cycles (SDLC) or new develop- ment techniques (i.e., prototyping, end-user computing, rapid systems, or application development)
- Reporting to management and performing a follow-up review to ensure actions taken at work

The auditing of IT and communications protocols typically involves the Internet, intranet, extranet, electronic data interchange, client servers, local and wide area networks, data communications, telecommunications, wireless technology, integrated voice/data/video systems, and the software and hardware that support these processes and functions. Some of the top reasons to initiate an IT audit include the increased dependence on information by organizations, the rapidly changing technology with new risks associated with such technology, and the support needed for financial statement audits.

SOX also requires the assessment of internal controls and makes it mandatory for SEC registrants. As part of the process for assessing the effectiveness of internal controls over financial reporting, management needs to consider controls related to the IS (including technologies) that support relevant business and financial processes. These controls are referred to as ITGCs (or IT general controls). As mentioned earlier, ITGCs are IT processes, activities, and/or procedures that are performed within the IT environment and relate to how the applications and systems are developed, maintained, managed, secured, accessed, and operated. Exhibit 1.4 illustrates other top reasons to have IT audits.



To assess the increase of sophisticated and "creative" programming

To support the effective functioning of application controls

To support financial statement audits

To control and monitor the significant growth of corporate hackers, either internal or external

To assess the completeness and accuracy of information

To address the rapidly changing technology and the new risks associated with such technology

To assess the integrity of information and security of data

To identify controls that can address specific IT risks

To control the easy access to organization networks from office and remote personal computers

To audit large amounts of data

Exhibit 1.4 Top reasons for having an IT audit.

Role of the IT Auditor

As the use of IT in organizations continues to grow, auditing computerized systems must be accomplished without many of the guidelines established for the traditional auditing effort. In addition, new uses of IT introduce new risks, which in turn require new controls. IT auditors arein a unique position to evaluate the relevance of a particular system to the enterprise as a whole. Because of this, the IT auditor often plays a role in senior management decision making.

The role of an IT auditor involves developing, implementing, testing and evaluating audit review procedures. You'll be responsible for conducting IT and IT-related audit projects using the established IT auditing standard in your organization. The audit process can extend to networks, software, programs, communication systems, security systems and any other services that rely on the company's technological infrastructure.

It's an essential role for organizations that rely on technology given that one small technical error or misstep can ripple down and impact the entire company. IT audits are important for evaluating internal control and processes in an effort to keep the organization and its data secure from external or internal threats.

The IT auditor's role has evolved to provide assurance that adequate and appropriate controls are in place. Of course, the responsibility for ensuring that adequate internal controls are in place rests with the management. The audit's primary role, except in areas of management advisory services, is to provide a statement of assurance as to whether adequate and reliable internal controls are in place and are operating in an efficient and effective manner.

Therefore, whereas management is to ensure, auditors are to assure.

IT Audit Responsibilities

As an IT auditor you will be responsible for running several audits of an organization's technologies and processes. IT audits are also referred to as automated data processing (ADP) audits and computer audits. In the past, IT audits have also been labeled as electronic data processing (EDP) audits. Companies may also run an information security (IS) audit to evaluate the organization's security processes and risk management. The IT audit process is typically utilized to asses data integrity, security, development and IT Governance.

There are several types of IT audits, including:

- Technological innovation process: an audit process that creates a risk profile for current and future projects with a focus on the company's experience with those technologies and where it stands in the market
- Innovative comparison audit: an audit that looks at an organization's ability to innovate compared to competitors and evaluates how well the company produces new products
- Technological position audit: an audit that examines current technology in the organization and future technologies that will need to be adopted
- Systems and applications: an audit process that specifically evaluates whether systems and applications are controlled, reliable, efficient, secure and effective
- Information processing facilities: an audit to evaluate an organization's ability to produce applications even in disruptive conditions
- Systems development: an audit for verifying that systems that are being developed are suited for the organization and meet development standards
- Management of IT and enterprise architecture: an audit of the IT management's organizational structure for information processing
- Client, server, telecommunications, intranets and extranets: audits to examine controls on client-connected servers and networks

References:

Information Technology Control and Audit, Fifth Edition, 2019 by Taylor & Francis Group, LLC

CRC Press is an imprint of Taylor & Francis Group

http://www.taylorandfrancis.com