LECTURE 7 & 8

AUDITOR & IT AUDIT

Dr WarusiaMohamed Yassin

PART A

Internal & External Audit

An Internal Audit:

- Is a company personnel that reporting to management or the audit committee of board of directors.
- Can be external for the department or division that being audited.
- Ensure an employee adherence to company policies, procedures and evaluation of internal controls.

An External Audit:

- Carried out by an external party
- Auditing various scope of services such as financial statements, information technology and many more.

IT Audit Group

General Computer Control Audit:

- It examines IT general controls 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: data backup, offsite storage, access to the job scheduler and etc.
    2. Information security (ISec): access and request user account information, access termination, and physical security.
    3. Change control management (CCM): application and database upgrade, security, network infra monitoring and etc.

IT Audit Group

Application Control Audit:

- It examines processing controls specific to the application that 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.

Relationship between general computer controls and application controls.

Why need 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

Otero, A.R., Information Technology Control and Audit, Fifth Edition, CRC Press, 2018.

- 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
  - Reporting to management and performing a follow-up review to ensure actions taken at work

Information Technology Auditor Role

- The auditor evaluating today's complex systems must have highly developed technical skills to understand the evolving methods of information processing.
- Contemporary systems carry risks such as non-compatible platforms, new methods to penetrate security through communication networks (e.g., the Internet), and the rapid decentralization of information processing with the resulting loss of centralized controls.
- 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.
- IT auditor often plays a role in senior management decision making. The role of IT auditor can be examined through the process of IT governance and the existing standards of professional practice for this profession.
- As mentioned earlier, IT governance is an organizational involvement in the management and review of the use of IT in attaining the goals and objectives set by the organization.

Information Technology Auditor Role

IT Auditor as Counsellor

- IT auditors must take an active role in assisting organizations in developing policies, procedures, standards, and/or best practices on safeguarding of the information, auditability, control, testing, etc.
- A good information security policy, for instance, may include:
  - ✓ Specifying required security features
  - ✓ Defining "reasonable expectations" of privacy regarding such issues as monitoring people's activities
  - ✓ Defining access rights and privileges and protecting assets from losses, disclosures, or damages by specifying acceptable use guidelines for users
  - ✓ Providing guidelines for external communications (networks)
  - ✓ Defining responsibilities of all users
  - ✓ Establishing trust through an effective password policy
  - ✓ Specifying recovery procedures
  - ✓ Requiring violations to be recorded

Information Technology Auditor Role

IT Auditor as Partner of Senior Management

- Although the IT auditor's roles of counselor and skilled technician are vital to successful company operation, they may be irrelevant if the auditor fails to view auditing in relation to the organization as a whole.

- Decisions concerning the need for a system traditionally belonged to management, but because of a combination of factors (mostly the complex technology of the computer), computer system audits were not successfully performed.

Information Technology Auditor Role

- When allocating funds for new systems, management has had to rely on the judgment of computer personnel.
- IT auditors have to provide management with an independent assessment of the effect of IT decisions on the business.
- In addition, the IT auditor can verify that all alternatives for a given project have been considered, all risks have been accurately assessed, the technical hardware and software solutions are correct, business needs will be satisfied, and costs are reasonable.

Information Technology Auditor Role

IT Auditor as Investigator

- As a result of increased legislation and the use of computer evidence within the courts, the ability to capture and document computer-generated information related to criminal activity is critical for purposes of prosecution.

- The awareness and use of computer-assisted tools and techniques in performing forensic support work have provided new opportunities for the IT auditor, IT security personnel, and those within law enforcement and investigation.

Information Technology Auditor Role

- The IT auditor can work in the field of computer forensics or work side by side with a computer forensics specialist, supplying insight into a particular system or network.

- Although the specialist is highly trained and can adapt to almost any system or platform, collaboration can make the jobs of the forensic specialist and the IT professional easier and more efficient.

Information Technology 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 is constantly evolving and finding ways to shape today's IT environment in the organization such as cloud computing, big data, IoT, block chain, autonomous vehicles and many more.

IT Environment as A Part of Organization Strategy

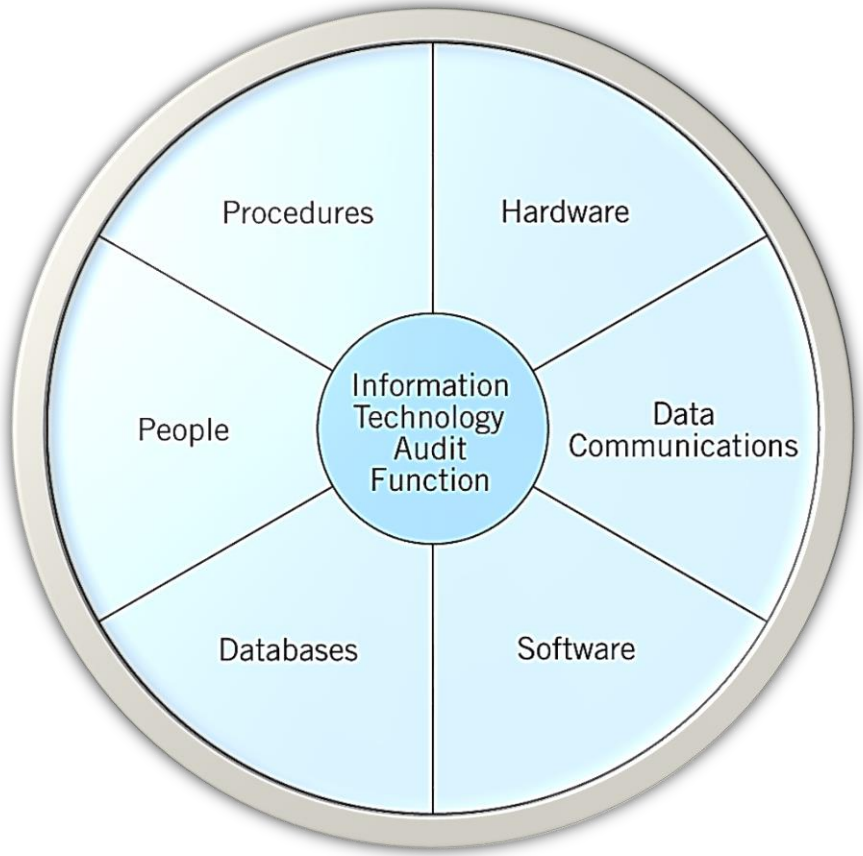
- In today's environment, organizations must integrate their IT with business strategies to attain their overall objectives.
- Today IT regarded as an integral part of that strategy to attain profitability and service.
- Besides, issues such as IT governance, international information infrastructure, security, and privacy and control of public and organization information have driven the need for self-review and self-assurance.

IT Environment as A Part of Organization Strategy

- For the IT manager, the words “audit” and “auditor” send chills up and down the spine.
- 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.
- 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.

Information Technology Auditing

- Generally, focuses in evaluating the computing role in achieving audit and control objectives
- Ensures and proving data and information are reliable, secure, confidential and available when required.
- Other focuses are mainly for safeguarding an assets and data integrity, as well as operational effectiveness.



Otero, A.R., Information Technology Control and Audit, Fifth Edition, CRC Press, 2018.

Information Technology Audit Process

- Example: Computer-assisted audit techniques (CAATs) are used when:

✓ Controls are weak for substantive testing of transactions and account balances.

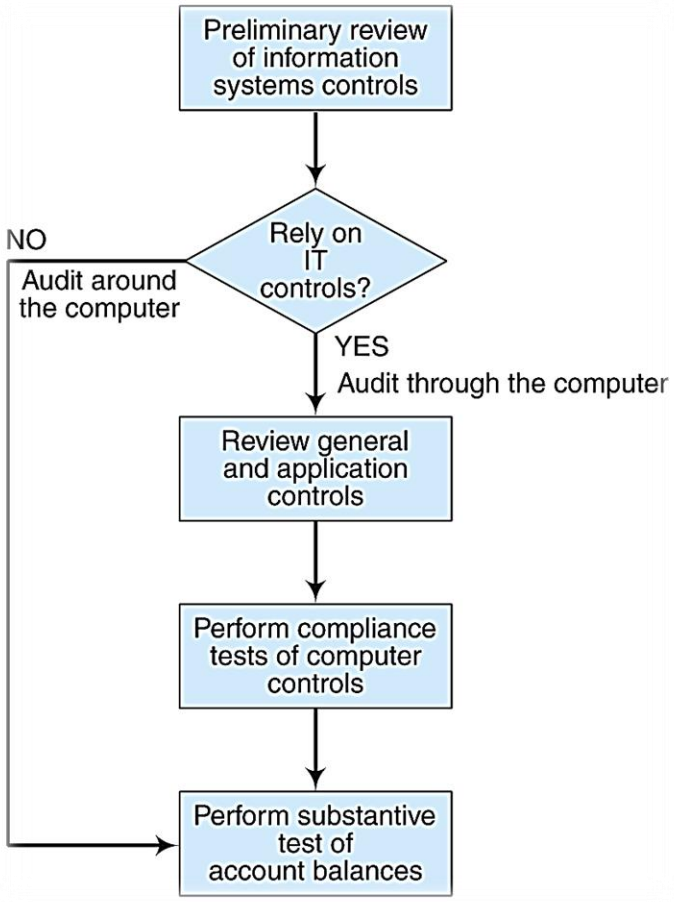
✓ Controls are strong for compliance testing to ensure controls are in place and working as prescribed.

Information Technology Audit Process

- Example: Computer-assisted audit techniques (CAATs) are used when:

✓ Controls are weak for substantive testing of transactions and account balances.

✓ Controls are strong for compliance testing to ensure controls are in place and working as prescribed.



Otero, A.R., Information Technology Control and Audit, Fifth Edition, CRC Press, 2018.

Career in Information Technology Auditing

- The demand for IT auditors is growing day by day as the technology become more advanced and complex such as big data, cloud, IoT and many more.
- Thus, variety IT auditing skills is required i.e., information system, computer science, computer security, computer forensic and many more.
- An auditor can be internal or external that usually have several professional certificate qualification.
- For example, Certified Information System Auditor (CISA), Certified Information Security Managers (CISM), Certified Information Security Management System (ISMS) Auditor.

Career in Information Systems Auditing

- Internal auditor
- Public accounting auditor
- IS analyst
- IT audit manager
- IT project manager
- IT security officer
- Network operation security engineer
- Cyber security professional
- IT consultant
- IT risk and assurance manager
- Privacy officer
- Chief information officer

Otero, A.R., Information Technology Control and Audit, Fifth Edition, CRC Press, 2018.

PART B

Auditing IT Environment

- Application systems provide automated functions to effectively support the business process.
- Besides, applications also introduce risks to organizations in the form of increased costs, loss of data integrity, weaknesses in confidentiality, lack of availability, and poor performance, among others.
- Moreover, once implemented, applications may be periodically modified to either correct errors or just implement upgrades and enhancements (maintenance).
- Such maintenance will need to be consistent with business or IT strategies; otherwise, it may cause performance issues and inefficient use of resources.

Auditing IT Environment

Application Systems Risk

- Concentrated data in a format increases the risks by placing greater reliance on a single piece of data or on a single computer file or on a database table.
- Similarly, the higher the number of applications that use the concentrated data, the greater the impact when that data become unavailable due to hardware or software problems.
- In fact, having a single database improves the quality and timeliness of financial information, but processing errors can quickly impact multiple functions as the information is shared but sourced from the same database.

Auditing IT Environment

Application Systems Risk

- Modifications (i.e., software releases) require considerable programming to retrofit all of the organization-specific code.
- Packaged systems are generic by nature, thus, organizations may need to modify their business operations to match the vendor's method of processing, for instance.
- Changes in business operations may not fit well into the organization's culture or other processes, and may also be costly due to training.
- Application systems like ERP systems are frequently exposed to many types of risks. Additional common risks associated with application systems include:

Auditing IT Environment

Application Systems Risk

- Weak information security
- Unauthorized access to programs or data
- Unauthorized remote access
- Inaccurate information
- Erroneous or falsified data input
- Incomplete, duplicate, and untimely processing
- Communications system failure
- Inaccurate or incomplete output
- Insufficient documentation

Auditing IT Environment

Application Systems Risk ***(Weak information security)***

- Information security should be a concern of IT, users, and management and yet not been a consistent top priority for many organizations.

- Past surveys and reports have shown that organizations are more concerned with budgets and staff shortages than information security.

- Respondents to such surveys still continue to identify obstacles to reducing information security risks, such as lack of human resources, funds, management awareness, and tools and solutions.

- Meanwhile, advanced technology and increased end-user access to critical and sensitive information continue to proliferate information security risks.

Auditing IT Environment

Application Systems Risk ***(Unauthorized access to programs or data)***

- Application systems should be built with various levels of authorization for transaction submission and approval.

- Once an application goes into production, programmers should no longer have access to programs and data or if programmers are provided access, such access should be a "read-only" access for the purpose of understanding issues reported by the user.

- Similarly, users' access should be limited to a "need-to-know" basis, means that the information made available to a user, whether it is "read-only" or with open access for modification, should be in accordance with the user's job functions and responsibilities.

Auditing IT Environment

Application Systems Risk ***(Unauthorized remote access)***

- Remote access allows users within an organization to access its network and computer resources from locations outside the organization's premises.

- Remote access, if unauthorized, does represent a risk because **client devices** (used for the remote access) tend to have weaker protection than standard or organization-based client devices.

- For example, remote access communications may be carried over untrusted networks, subjecting the communication to unauthorized monitoring, loss, or manipulation.

- User access reviews should be periodically performed by IS security personnel, and approved by management, to ensure the remote access granted is accurate and consistent.

Auditing IT Environment

Application Systems Risk ***(Inaccurate information)***

- Accurate information must be ensured whether the end user is accessing data from an application, a departmental database, or information on the cloud.

- Departmental **data repositories** (e.g., databases, data clouds, etc.) may have redundant information with different timeframes and result in waste of time in reconciling these repositories to determine which data are accurate.

- Another major area of concern is that management may fail to use information properly due to failures in identifying significant information; interpreting meaning and value of the acquired information; and/or communicating critical information to the responsible manager or chief decision maker on a timely basis.

Auditing IT Environment

Application Systems Risk ***(Communications system failure)***

- Today, application systems within IT environments are responsible for many critical services, including communication services (e.g., e-mail, intranets, Internet, instant messaging, etc.).

- Because of this increasing reliance on IT communication services, the potential failure of these services presents an increasing source of risk to organizations.

- Information that is routed from one location to another over communication lines is vulnerable to accidental failures, intentional interception, and/or modification by unauthorized parties.

Auditing IT Environment

End-user Development Risks

- End-user development (EUD) (also known as end-user computing) generally involves the use of department-developed applications, such as spreadsheets and databases, which are frequently used as tools in performing daily work.

- These spreadsheets and databases are essentially an extension of the IT environment and output generated from them may be used in making business decisions impacting the company.

- The level of risk and the required controls to be implemented depend on the criticality of the EUD application.

- For example, an EUD application that consolidates data from several departments that will later be an input into the financial reporting system is a prime target for an audit. levels of controls.

Auditing IT Environment

End-user Development Risks

- Risks associated with EUD application systems include:
  - Higher organizational costs
  - Incompatible systems
  - Redundant systems
  - Ineffective implementations
  - Absence of segregation of duties
  - Incomplete system analysis
  - Unauthorized access to data or programs
  - Copyright violations
  - Lack of back-up and recovery options
  - Destruction of information by computer viruses

Auditing IT Environment

End-user Development Risks *(higher organizational costs)*

- EUD may at first appear to be relatively inexpensive compared to traditional IT development.
- However, a number of hidden costs are associated with EUD that organizations should consider.
- In addition to operation costs, costs may increase due to lack of training and technical support.
- Lack of end-user training and their inexperience may also result in the purchase of inappropriate hardware and the implementation of software solutions that are incompatible with the organization's systems architecture.

Auditing IT Environment

End-user Development Risks *(Incompatible systems)*

- End-user-designed application systems that are developed in isolation may not be compatible with existing or future organizational IT architectures.

- Traditional IT systems development verifies compatibility with existing hardware and related software applications.

- The absence of hardware and software standards can result in the inability to share data with other applications in the organization.

Auditing IT Environment

End-user Development Risks *(Redundant systems)*

- In addition to developing incompatible systems, end users may be developing redundant applications or databases because of the lack of communication between departments.

- Because of this lack of communication, end-user departments may create a new database or application that another department may have already created.

- A more efficient implementation process has enduser departments coordinating their systems development projects with IT and meeting with other end-user departments to discuss their proposed projects.

Auditing IT Environment

End-user Development Risks ***(unauthorized access to data or programs)***

- Access controls provide the first line of defense against unauthorized users who gain entrance to an application system's programs and data.

- The use of access controls, such as user IDs and passwords, are typically weak in user-developed systems and in some cases, user IDs and passwords may not even be required, or they would be very simple and easily guessed.

- This oversight can subject applications to accidental or deliberate changes or deletions that threaten the reliability of any information generated.

- To prevent any accidental changes, the user should be limited to execute only.

Auditing IT Environment

End-user Development Risks (Copyright violations)

- Organizations are responsible for controlling the computing environment to prevent **software piracy** and copyright violations.
- However, some organizations may not specifically address software piracy in training, in policy and procedures, or in the application of general internal controls.
- Since software programs can easily be copied or installed on multiple computers, many organizations are in violation of copyright laws and are not even aware of the potential risks.
- Organizations should inform end users of the copyright laws and the potential consequences that result from violations of those laws and prevent installation of unauthorized software.

Auditing IT Environment

End-user Development Risks (lack of back-up and recovery options)

- Nowadays, it is extremely easy to lose data and all but impossible to rebuild that data if backups had not been performed.
- In case of a disaster or virus attack, applications (and their data) may not be recoverable because of the lack of backups.
- The absence of a back-up and recovery strategy results in computer data loss.
- Unbacked up data is constantly subject to risks, such as accidental deletion of files, viruses and damaging malware, hard drive failures, power failures or crashes, theft of computer, water damage, fire, and many others.

Auditing IT Environment

End-user Development Risks ***(destruction of information by computer viruses)***

- Most end users are knowledgeable about computer virus attacks, but the effect of a virus remains only a threat until they actually experience a loss.

- Viruses can cause a variety of problem such as, destroying or altering data, destroying hardware, slowing down a network by performing many tasks that are really just a continuous loop with no end or resolution, producing spamming and launching denial-of-service attacks

- The risk to organizations is the time involved in removing the virus, rebuilding the affected systems, and reconstructing damaged data.

- Viruses cause significant financial damage, and recipients may file lawsuits against the instituting organization.

Auditing IT Environment

Risks to Systems Exchanging Electronic Business Information

- Electronic Data Interchange (EDI) refers to the electronic exchange of business documents between business (or trading) partners using a standardized format.
- EDI allows organizations to electronically send and receive information in a standard format so that computers are able to read and understand the documents being interchanged.
- A standard format describes the type, as well as the design, style, or presentation (e.g., integer, decimal, mmddyy, etc.) of the information being traded.
- Exhibit 9.1 describes risks associated with EDI or systems exchanging electronic business information.

Risks to Systems Exchanging Electronic Business Information

Risk	*Description*
Loss of business continuity/going-concern problem	Inadvertent or deliberate corruption of EDI-related applications could affect every EDI transaction entered into by an organization, impacting customer satisfaction, supplier relations, and possibly business continuity eventually.
Interdependence	There is increased dependence on the systems of trading partners, which is beyond the control of the organization.
Loss of confidentiality of sensitive information	Sensitive information may be accidentally or deliberately divulged on the network or in the mailbox storage system to unauthorized parties, including competitors.
Increased exposure to fraud	Access to computer systems may provide an increased opportunity to change the computer records of both a single organization and that of its trading partners by staff of the trading parties or by third-party network staff. This could include the introduction of unauthorized transactions by user organization or third-party personnel.
Manipulation of payment	A situation where amounts charged by or paid to suppliers are not reviewed before transmission. Therefore, there is a risk that payments could be made for goods not received, payment amounts could be excessive, or duplicate payment could occur.
Loss of transactions	Transactions could be lost as a result of processing disruptions at third-party network sites or en route to the recipient organization, which could cause losses and inaccurate financial reporting.

Risk	*Description*
Errors in information and communication systems	Errors in the processing and communications systems, such as incorrect message repair, can result in the transmission of incorrect trading information or inaccurate reporting to management.
Loss of audit trail	EDI eliminates the need for hard copy. There will be less paper for the auditors to check. The EDI user may not provide adequate or appropriate audit evidence, either on hard copy or on electronic media. The third-party vendor may not hold audit trails for a significant length of time, or audit trails could be lost when messages are passed across multiple networks.
Concentration of control	There will be increased reliance on computer controls where they replace manual controls, and they may not be sufficiently timely. The use of EDI with its greater reliance on computer systems concentrates control in the hands of fewer staff, increases reliance on key people, and increases risk.
Application failure	Application or EDI component failures could have a significant negative impact on partner organizations within the respective business cycles, especially for **Just-In-Time inventory** management, production, and payment systems. In addition, there is a possibility of error propagation across other systems due to integration with other business applications.
Potential legal liability	A situation where liability is not clearly defined in trading partner agreements, legal liability may arise due to errors outside the control of an organization or by its own employees. There is still considerable uncertainty about the legal status of EDI documents or the inability to enforce contracts in unforeseen circumstances.

Otero, A.R., Information Technology Control and Audit, Fifth Edition, CRC Press, 2018.

Auditing IT Environment

Risks to Systems Exchanging Electronic Business Information

- Implications arising from these risks include:
  - Potential LOSS of transaction audit trail, thereby making it difficult or impossible to reconcile, reconstruct, and review records. This could possibly be a breach of legislation and result in prosecution and fines.
  - Increased exposure to ransom, blackmail, or fraud through potential disruption of services or increased opportunities to alter computer records in an organization and its trading partners' IS.
  - Disruption of cash flows when payment transactions are generated in error or diverted or manipulated.
  - Loss of profitability occurring through increased interest charges or orders going to a competitor due to lack of receipt of EDI messages.
  - Damage to reputation through loss of major customers, especially if EDI problems are widely publicized.

Auditing IT Environment

Web Application Risks

- From a development point of view, a Web application should be designed to perform the specific tasks agreed upon and documented as part of the functional requirements.

- When developing Web applications, teams must understand that client-side controls like input validation, hidden fields, and interface controls, for example, are not fully dependable for security purposes.

- Attackers may easily bypass these client-side controls and gain access to analyze or manipulate application traffic, submit requests, etc.

- Well-known practices need to be concern in developing Web application systems or applications such as Open Web Application Security Project (OWASP) Secure Coding Guidelines.

Auditing IT Environment

Example to Remediate Web Application Risks

- Input validation
- Output encoding
- Authentication and password management
- Session management
- Access control
- Cryptographic practices
- Error handling and logging
- Data protection
- Communication security
- System configuration
- Database security
- File management
- Memory management
- General coding practices

Auditing IT Environment

Web Application Risks

- Example: Injection, Broken authentication and session management, Cross-site scripting, Broken access control, Security misconfiguration, Sensitive data exposure, Insufficient attack protection, Cross-site request forgery, Using components with known vulnerabilities and Under protected application program interfaces.

- The OWASP secure coding principles and practices checklist is one effective way to minimize risks and ensure that the organization develops successful Web applications.

- However, auditors, management, developers, and security consultants must consider the levels of risks associated with all types of applications in order to design and implement appropriate application controls.

Auditing IT Environment

IT Auditor's Involvement

- IT auditors can assist organizations by reviewing their application systems to ensure they comply with the organization's strategy and standards, as well as provide automated functions to effectively support the business process.

- Applications will need to be risk assessed to determine the level of audit involvement and the type of assessment will also vary depending on the risks of the particular application.

- Applications introduce risks to organizations in the form of increased costs, loss of data integrity, weaknesses in confidentiality, lack of availability, poor performance, and others.

- These risks should be addressed with adequate selection and implementation of controls.

Auditing IT Environment

IT Auditor's Involvement

- Auditing application systems requires specific knowledge about application risks and controls and understanding those allows the IT auditor to identify key areas that would benefit from independent verification.

- Moreover, understanding application controls allows the IT auditor to evaluate and recommend the ones that will ensure complete and accurate transaction processing.

- Results from the risk assessment also prompt the amount of time necessary to allocate to the particular application, required resources, etc.

- IT auditors finally communicate findings identified throughout the audit plus recommendations to management.

Auditing IT Environment

IT Auditor's Involvement (*Risk Assessment)*

- IT auditors may not have enough time to assess every particular application system in the organization and involvement within a particular application will depend on the assessment of the application risks.
- Application risks relate to application complexity and magnitude, inexperienced staff, lack of end-user involvement, and lack of management commitment.
- The level of risk may be a function of the need for timely information, complexity of the application, degree of reliance for important decisions, length of time the application will be used, and the number of people who will use it.
- The risk assessment defines which aspects of a particular application will be covered by the audit and the scope of the audit may vary depending on the risks identified.

Auditing IT Environment

IT Auditor's Involvement (*Audit Plan)*

- **The audit plan** details the steps and procedures to fulfill the audit objectives.
- As in any audit, an audit of application systems begins with a preliminary analysis of the control environment by reviewing existing standards, policies, and procedures.
- During the audit, these standards, policies, and procedures should be assessed for completeness and operational efficiency.
- The preliminary analysis should identify the organization's strategy and the responsibilities for managing and controlling applications. Documenting an understanding of the application system is also a must at this stage.

Auditing IT Environment

IT Auditor's Involvement

- The audit plan will further document the necessary procedures to carry on the examination to ensure that the application system is designed and implemented effectively, as well as operates consistent with the organization policies and procedures.

- Procedures performed by IT auditors should provide reasonable assurance that applications have been adequately designed and implemented, and:

  - Comply with standards, policies, and procedures
  - Achieve efficient and economical operations
  - Conform to legal requirements
  - Include the necessary controls to protect against loss or serious errors
  - Provide controls and audit trails needed for management, auditor, and for operational review purposes

Auditing IT Environment

IT Auditor's Involvement ***(Communication)***

- It is very important to make sure that management's expectations of the IT auditor's role are understood and communicated to all participants.

- IT auditors must develop an open line of communication with both management and users. If a good relationship between these groups does not exist, information might be withheld from the IT auditor.

- Throughout the audit, the IT auditor will be making control recommendations resulting from identified findings.

- Depending on the organization's culture, these recommendations may need to be handled informally with each application owner in charge of the deficient area or process, or formally by presenting them to the steering committee.

Auditing IT Environment

IT Auditor's Involvement ***(Communication)***

- In either case, the IT auditor must always consider the value of the control recommendation versus the cost of implementing the control.
- Recommendations should be specific.
- They should identify the problem and not the symptom, and allow for the proper controls to be implemented and tested.
- Findings, risks as a result of those findings, and audit recommendations are usually documented in a formal letter (i.e., Management Letter).