Information Systems and Cyber Security Audit

Research submitted for participation in the 14th ARABOSAI Scientific Research Competition

Prepared by

Dr. Samy Ali M. Zaghloul

General Manager

Accountability State Authority

Arab Republic of Egypt

Acknowledgements

Praise be to Allah as befits His Majesty and His Great Power, and peace and blessings be upon our prophet Muhammad, may God bless him and grant him peace, and upon his family and companions, and after.....

I extend my sincere thanks and appreciation to both H.E. President of the Accountability State Authority(ASA) and H.E. the ASA Vice President for their constant encouragement of the ASA members to conduct scientific research and participate in scientific competitions as well as contribute to local and international scientific forums, as this enhances the competencies, skills and capabilities of the ASA members. My thanks are extended to all those who helped me in completing this work; namely the ASA heads and members.

I also extend my sincere gratitude to the Arab Organization of Supreme Audit Institutions (ARABOSAI) Officials and the members of the Institutional Capacity Building Committee for their efforts in constantly encouraging the Arab SAIs' members to conduct scientific research, as this has a great impact on enhancing their ongoing scientific and professional qualification, which ultimately leads to improving the quality of their auditing performance in tasks they perform, which benefits their countries.

Researcher

Dr. Sami Ali Mohamed Zaghloul

Abstract

This research aims to identify the role of information security audit in limiting the risks of electronic information systems in governmental institutions, along with the associated auditing of information technology and the role of the Supreme Audit Institutions (SAIs). A questionnaire was designed to collect data and was distributed to a sample from SAI Egypt's members, audit firms as well as from employees of financial departments, internal audit and information technology in some Egyptian banks. The researcher followed both descriptive and analytical methodologies as they suit the research nature.

The researcher reached several conclusions, the most importqnt of which are:

- There is a statistically significant relationship between information security audit policies and their dimensions (system validity, audit team duties, internal audit system reports, documentation and evidence, Code of Conduct for information security auditing, external auditing) in limiting the risks of electronic information systems in Egyptian banks.
- The regular application of information technology systems auditing processes can significantly reduce cybersecurity risks and data breaches, thus enhancing the security of electronic information systems.
- The importance of having a strong and independent regulatory framework for information systems auditing, where SAIs can play a key role in identifying security standards and practices, monitoring their implementation and guiding organizations to improve the security and reliability of their systems. Collaboration between the public and private sectors can also enhance the effectiveness of oversight efforts and improve information security.
- Organizations should deal with various challenges related to information technology auditing, such as the evolving of cyber threats and new legislations related to data protection. One of the important opportunities is leveraging advancements in modern technology to enhance the ability of relevant entities to detect and combat security threats.
- Companies and institutions should adopt multiple strategies to improve information technology auditing processes, including

employing qualified cadres, adopting big data analytics techniques and collaborating with specialized security service providers.

The researcher proposes the following recommendations:

- Enhancing employees' awareness and training them:
  Organizations should enhance their employees' awareness of the importance of information security and safe technology practices as well as provide them with ongoing training on cyber threats and how to deal with them.
- Implementing regular auditing procedures: Organizations should conduct regular auditing of their systems and technologies to ensure their aligning with the latest security standards and complying with legislations and regulations.
- Strengthening cooperation with SAIs: Organizations should enhance cooperation with SAIs and leverage the guidance and directives they provide to improve information security.
- Adopting best practices and modern technologies: Organizations should use best practices and adopt modern technologies in implementing auditing processes and securing electronic systems.

Key words:
Audit, IT audit, Information systems risks, Supreme Audit Institutions.

Table of Contents

Communication Technology Systems	
1/1/9Tasks of the Auditor of Information and Communication Technology Systems	
1/1/10 Legal Frameworks, Standards and Guides for Auditing Information and Communication Technology Systems	
1/1/11 Path of Auditing Information and Communication Technology Systems	
1/1/12Impact of Information and Communication Technology Systems on Audit Procedures	
1/1/13 Tools and Techniques for Auditing Information and Communication Technology	
1/1/14Areas of Auditing Information and Communication Technology Information	
1/1/15The role of supreme audit institutions in the field of IT auditing	
1/1/16Experiences of supreme audit institutions in IT auditing	
1/1/17 Common observations in IT auditing	
1/1/18Challenges facing IT auditing	
1/1/19Confronting the challenges facing IT auditing	
Section Two: Risks of electronic information systems	
1/2/1 Introduction	
1/2/2 The concept of electronic information systems	
1/2/3 Objectives of electronic information systems	
1/2/4 Characteristics of electronic information systems	
1/2/5 The role of electronic information systems in decision-making and taking	
1/2/6 Electronic accounting information systems	
1/2/7Types of risks facing electronic information systems	
1/2/8Causes of risks facing electronic information systems	

List of Tables

Table of Figures

Introductory Chapter
General Framework of the Research and Previous Studies

Introductory Chapter
General Framework of the Research and Previous Studies

First: Introduction

In the era of modern digital technology, information technology has facilitated and continues to facilitate life in general and the world of finance and business in particular. The need arose to leverage the capabilities of information systems and communication networks; information systems and information technology have become essential to the success of any organization or institution.

The great reliance on information technology has resulted in major changes in the components of information systems; in terms of changing the design and composition of these systems, their production of many new risks, their lack of a visual audit path, changing the nature of proving evidence and creating others that are not distinguished by traditional systems, such as changing their internal control structure and its technical complexity that is compatible with the electronic environment of general control over the systems' environment and special control over electronic applications.

As auditing is a profession that is primarily based on issuing a neutral opinion supported by evidence about the fairness and credibility of accounting information that are the outputs of electronic information systems or are electronic in themselves; there is no doubt that this will require obtaining a comprehensive understanding of the nature and characteristics of these systems that produce this information and ensuring that control over the inputs, the electronic processing process and the resulting outputs are based on sound auditing controls, and that the electronic system contributes to protecting both data and information.

Because the auditor is guided in performing his work by professional standards, there is no doubt that this requires studying and evaluating the suitability of auditing standards with the new electronic environment, studying the possibility of relying on other standards outside the auditing standards that are concerned with the electronic aspect of information systems, or the possibility of relying on the computer itself as a tool in the auditing process (electronic auditing) in light of the development of specialized application programs in the field of auditing.

Information systems technology auditing and information security auditing are considered essential tools to ensure the safety and security of data and information in the digital era. In addition, SAIs are considered essential partners in enhancing trust and transparency as well as successfully achieving the Organization's goals.

Second: Previous Studies

Within the limits of the survey carried out by the researcher of related academic studies, which are relevant to the topic of his research, the researcher reviews a summary of these studies and their findings as follows:

Studies in Arabic

1. **Hashem's study, Heba Gamal, (2023), entitled: A Proposed Procedural Approach to Measure the Extent of the External Auditor's Response to Cyber Risks in the Client's Facility.**

   The study aimed to reach a proposed procedural approach to measure the extent of the external auditor's response to cyber risks in the client's facility in the Egyptian environment. The study addressed the repercussions of cybersecurity risks on the external auditor's work and the proposed approach's steps. The applied study methodology was based on joint-stock companies listed on the Egyptian Stock Exchange and operating in sectors and activities related to modern technologies in information systems and technology.

The study concluded that the assessment of cybersecurity risks depends on audit processes that study and evaluate a set of pre-determined controls in topics related to cybersecurity. The findings also showed a significant direct effect of the risks of cybersecurity attacks in the client's facility on the external auditor's work, and a significant direct correlation between the management of disclosure of cybersecurity risks and the proposed procedural approach for the external auditor's work.

2. **Al-Awamri, Abeer Issa's study (2022) entitled: The Impact of the Integration of Information Security Governance and Trust Assurance Services on Reducing the Risks of Electronic Accounting Information Systems.**

This study aimed to explore the impact of the integration of information security governance and trust assurance services on reducing the risks of electronic accounting information systems; in order to increase reliability and credibility in electronic accounting information systems and their outputs.

The study's finfings illustrated that electronic accounting information systems are exposed to many risks, the most important of which are internal risks. The most important reasons for the occurrence of these risks are the inefficiency and effectiveness of the information systems procedures and controls within the companies under study as well as the non-inclusion of a large number of the study sample to the objectives and principles of both information security governance and trust assurance services within their future strategy.

3. **Al-Azmi, Abdullah Faleh, (2022) study entitled: The Role of Activating Information Technology Governance in Securing Accounting Information from Electronic Risks in the Age of Digitization.**

The study aimed to identify the risks' nature which threatens the security of electronic accounting information systems in Kuwaiti banks, their recurrence rates and sources of occurrence.

The study's findings showed that electronic accounting information systems are exposed to many risks and that there is a significant influence of the impact of activating the dimensions of information technology governance on securing accounting information from electronic risks, and that following a sound accounting information system reduces the risks of electronic accounting information systems, and that leveraging global expertise in the field of information security raises the degree of confidence in electronic accounting information.

4. **Habib, Samar's study, 2022, entitled: The Role of Accounting and Cloud Auditing Standards in Ensuring Data and Information Security: A Field Study from the Perspective of External Auditors in Syria.**

The study aimed to survey the opinions of external auditors in Syria on the role of benefits and risks of cloud accounting and auditing when adopting cloud solutions and their opinions on the role of cloud auditing standards (SAS70, SSAE16, ISO295) in ensuring data and information security, in addition to surveying their opinions on the availability of data and information security controls issued by international professional bodies and organizations in the rules and instructions issued by the Syrian legislator.

The study reached several findings, including the existence of statistically significant differences in the opinions of external auditors on each of the role of the benefits and risks of cloud accounting and auditing when adopting cloud solutions, the role of cloud auditing standards in ensuring data and information security as well as the availability of data and information security controls in the regulations issued by the Syrian legislator.

Studies in English

1. **Study (2024) Mirwali Azizi & et al entitled: The Role of IT (Information Technology) Audit in Digital Transformation: Opportunities and Challenges.**

The study seeks to shed light on how institutions can harness IT auditing to promote the benefits of digital transformation while limiting the associated

risks as well as examine the opportunities and challenges facing organizations globally. Through a comprehensive literature review to dissect the evolving role, ways to improve and obstacles encountered, the study emphasizes the need for IT auditing to adapt to technological developments while overcoming complex challenges to maintain its effectiveness. Addressing cybersecurity and resource constraints requires proactive measures and strategic investments. Organizations can also promote the value of digital transformation by enhancing IT auditing through proactive initiatives and nurturing talent development.

2. **Yohannes Kurniawan & Archie Mulyawan, 2023 study entitled: The Role of External Auditors in Improving Cybersecurity of the Companies through Internal Control in Financial Reporting.**

   The study aimed to explore the role of external auditors in improving companies' cybersecurity in financial reporting through developing internal controls in technology-based processes by analyzing audit findings.

   The study confirmed that the growth of innovative technology affects the auditor's ability to help audit the findings and risk measurements of audit. However, the auditor's ability to apply technology to the audit performance has little effect.

3. **Mohammad Aljanabi & et al, 2023 study entitled: The Purpose of Cybersecurity Governance in the Digital Transformation of Public Services and Protecting the Digital Environment.**

   The study aimed to conduct a survey on cybersecurity governance and digital transformation and their importance in creating a digital environment free from hacking and data theft that serves all citizens in better organizing their lives by relying on artificial intelligence technologies.

   The study confirmed that cybersecurity is one of the challenges facing many governments during the development of hacking operations, malware and technologies that contribute to creating loopholes in computer networks and that heavy reliance on artificial intelligence technologies contributes to

developing the digital environment and preserving data because these technologies have the ability to study the behavior of unauthorized persons and malicious programs.

Third: Commenting on previous studies and the research gap

By auditing previous studies that the researcher was able to address in the study, the researcher extracts the findings shown in the following figure:

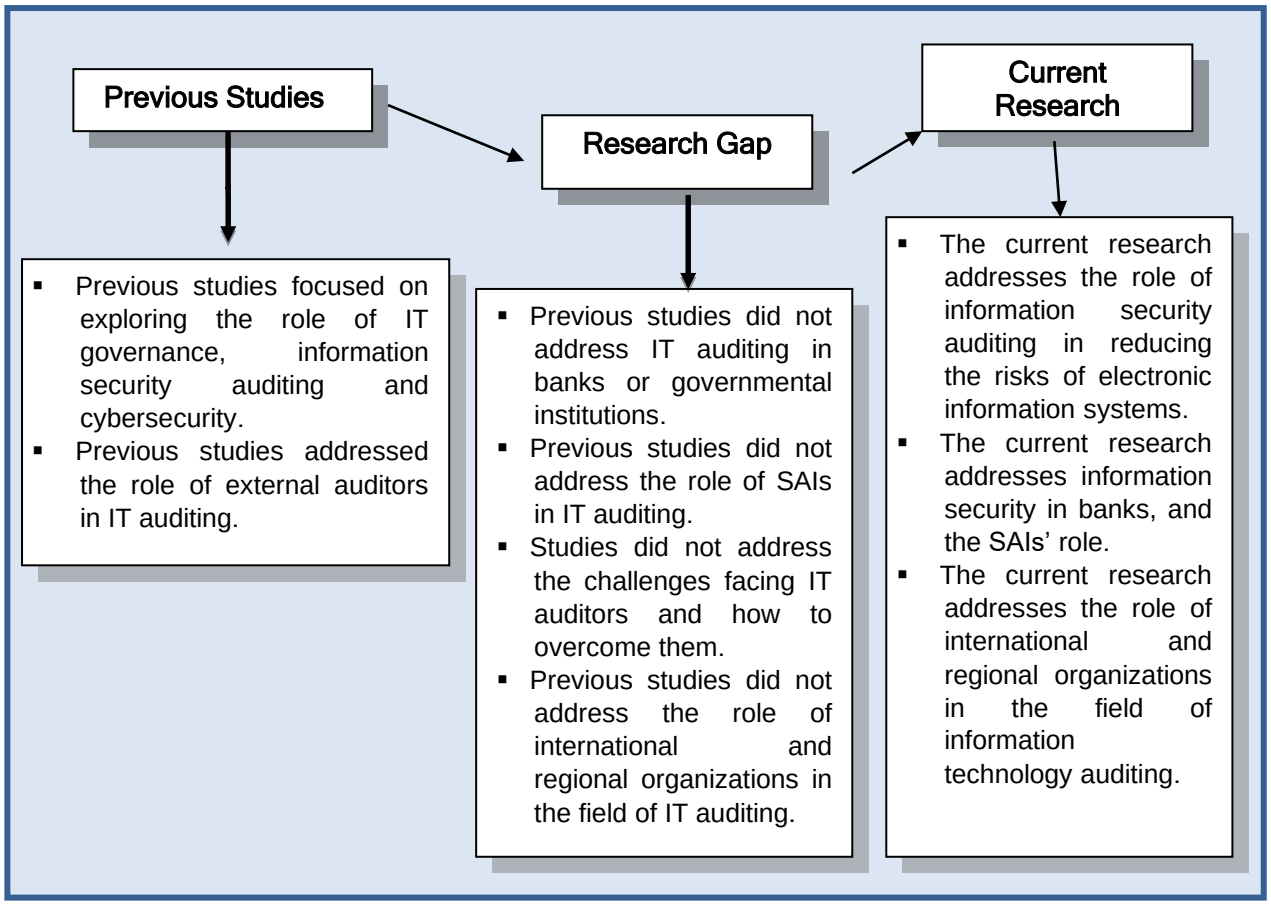


Figure No. (1): Comments on previous studies and the research gap

Source: By the researcher

It is clear from the previous figure that the researcher attempted in the current research to cover the research gap in previous studies and address the challenges facing IT auditors and how to overcome them as well as the role of professional organizations in this regard.

Fourth: Research problem

In light of the continuous development of information technology and the transition to digital environment, governmental organizations face increasing challenges regarding the security and integrity of data and information. Electronic information systems auditing and information security auditing are considered essential tools for assessing and improving data security in these organizations. However, despite of the importance of these tools, there remain specific challenges related to their application in the governmental environment.

Given this context, this study aims to analyze the impact of information security auditing on reducing the risks of electronic information systems in Egyptian banks and to provide the necessary recommendations to enhance the security of information and data in these banks.

Pertaining to the above, this research's problem is illustrated through the following question:

What is the role of information security auditing in reducing the risks of electronic information systems in Egyptian banks?

Fifth: Research variables

The study's variables are:

Independent variable: Information security audit policies.

Dependent variable: Electronic information systems risks.

Sixth: Structure of the research variables

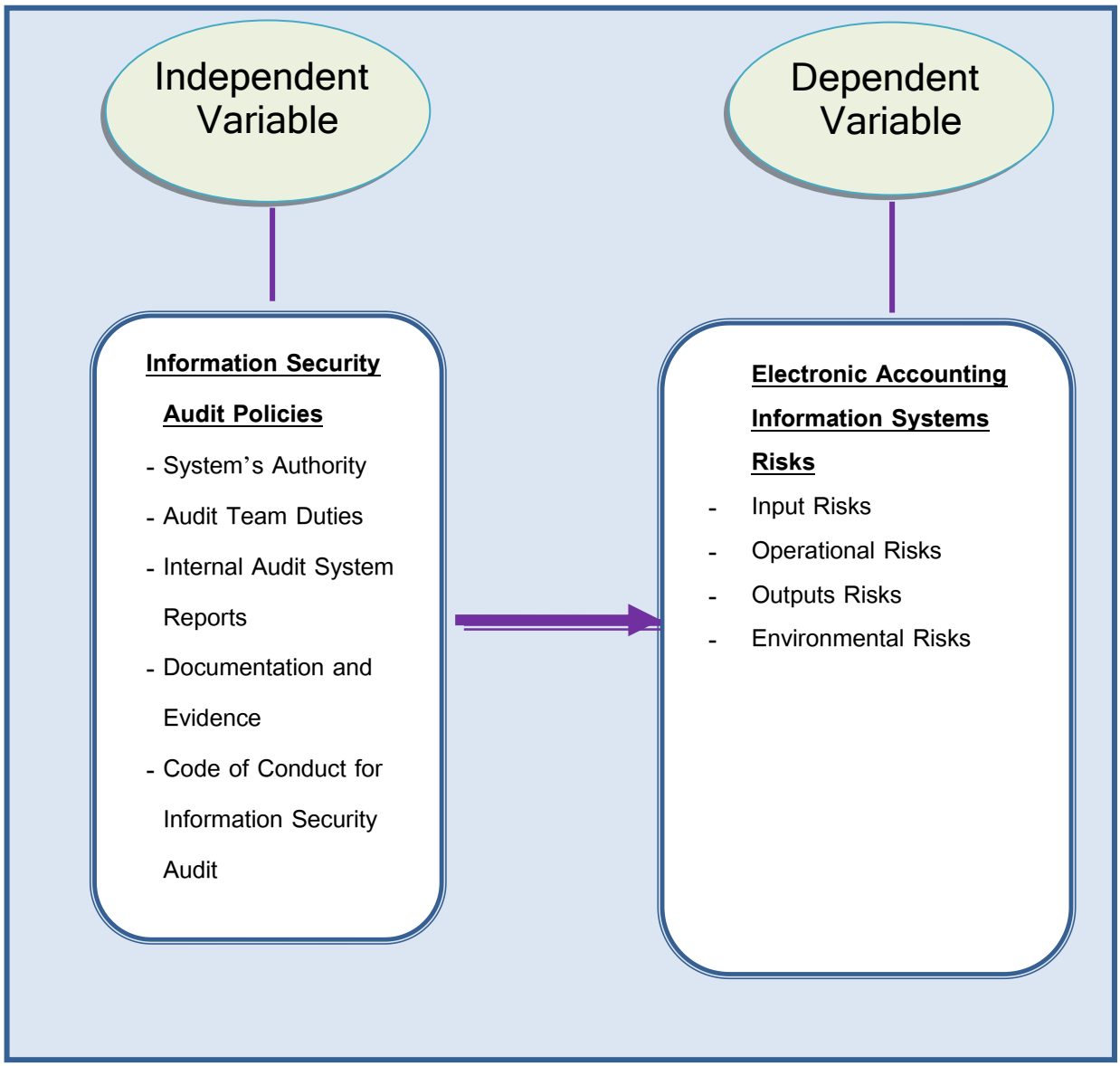


Figure No. (2): Structure of research variables

Source: By the researcher

Seventh: Research hypotheses

Based on the study's problem and its objectives, the main hypothesis can be formulated as follows:

There is a role for information security audit policies and their dimensions (system validity, audit team duties, internal audit system reports,

documentation and evidence, information security audit Code of Conduct, external audit) in reducing the risks of electronic information systems in Egyptian banks.

To achieve the research objective, the following hypotheses can be formulated:

First hypothesis:

There is a role for information security audit policies and their dimensions (system validity, audit team duties, internal audit system reports, documentation and evidence, information security audit Code of Conduct, external audit) in reducing the risks of entry in banks.

Second hypothesis:

There is a role for information security audit policies and their dimensions (system validity, audit team duties, internal audit system reports, documentation and evidence, information security audit Code of Conduct) in reducing operational risks in banks.

Third hypothesis:

There is a role for information security audit policies and their dimensions (system validity, audit team duties, internal audit system reports, documentation and evidence, information security audit Code of Conduct, external audit) in reducing outputs' risks in banks.

Fourth hypothesis:

There is a role for information security audit policies and their dimensions (system validity, audit team duties, internal audit system reports, documentation and evidence, information security audit Code of Conduct, external audit) in reducing environmental risks in banks.

Eighth: Research objectives

The objectives that the research seeks to achieve can be briefed as follows:

- Identifying the conceptual framework for information technology auditing.
- Identifying the risks of electronic information systems in government organizations.

- Analyzing the impact of information security auditing on reducing the risks of electronic information systems.
- Providing recommendations to enhance information security in government organizations.

By achieving these objectives, the study can contribute to enhancing information and data security in government organizations and providing practical guidance for applying best practices in the field of information systems auditing and information security.

Ninth: The importance of the research

The importance of the research – from the researcher's perspective – can be illustrated as follows:

From a scientific perspective

This research contributes to expanding scientific knowledge in the field of electronic information systems auditing and information security.It helps in understanding the relationship between information technology auditing and reducing information systems risks in government organizations.

This research also gains its scientific importance from the fact that it keeps pace with recent developments in the field of accounting researches that focuse on the impact of information technology on auditing and SAIs' role.

From a practical perspective

1. Providing practical guidance: This research provides practical guidance and methodologies for applying best practices in information systems auditing and information security in government organizations.
2. Enhancing security and trust: This research contributes to enhancing the security of information and data in government organizations, thus increasing trust in financial and administrative operations and reports.
3. Providing practical recommendations: This research helps in providing practical recommendations to government organizations to improve information security management and implement information security auditing in an effective manner.

In general, this research is important on both the scientific and practical levels, as it contributes to developing scientific knowledge and providing practical solutions to increase the security and reliability of electronic information systems in government organizations.

Tenth: Research method

To achieve the research objectives, the researcher used the descriptive and analytical methods, which rely on studying the reality or the phenomenon with an interest in describing it accurately and quantitatively. Through the use of the applied aspect, data and information were collected, and the available references, periodicals and the Internet were used to cover the theoretical aspect. The questionnaire was approved in the applied aspect as it is the main means, as its paragraphs were formulated in a manner consistent with the research variables by leveraging the studies mentioned in the theoretical aspect that addressed those variables. Simplicity and clarity were considered in formulating the questionnaire's paragraphs.

After collecting the necessary data from its various sources, whether primary or secondary data, this data was subjected to statistical analysis in order to extract a set of indicators with specific implications that are useful in testing hypotheses, revealing ambiguity in the research problem and achieving its objectives.

Eleventh: Research community and sample

The study community consisted of members of the Supreme Audit Institution in Egypt, employees of the financial sector, the Information Technology Sector, and the Internal Audit Sector in Egyptian banks belonging to the public sector. A random sample of 50 individuals was taken from the study community, represented by managers, external auditors, accountants, department heads, internal auditors and their assistants as well as information technology employees in the banks under study.

Twelfth: Research contents

To achieve the research objective and address its problem in a scientific manner, the research, in both its theoretical and applied aspects, included the following chapters:

Introductory Chapter: General framework of the research and previous studies

Chapter One: Conceptual framework for auditing electronic information systems

Topic One: Auditing information and communication technology

Topic Two: Risks of electronic information systems

Chapter Two: Applied study

Chapter Three: Findings and recommendations

References

Appendices

Chapter One
Conceptual Framework for Auditing Electronic Information Systems

Chapter One
Conceptual Framework for Auditing Electronic Information Systems

The successive developments in the field of information technology have brought about a major qualitative shift that has resulted in remarkable progress in the work patterns of business organizations, public and governmental sector organizations and bodies, and various aspects of life. This progress has contributed to radical changes in the information environment in various organizations. This has led to the emergence of various electronic information systems, which have facilitated operations and contributed to obtaining more accurate work findings in the least possible time and effort. However, this has been accompanied by obstacles that led to gaps in these systems' work, as many risks associated with electronic information systems have emerged, such as data entry risks, operational risks, outputs risks, environmental risks and other risks that might negatively affect the effectiveness of the system's performance and the desired objectives of its existence, which might be intentional or unintentional. This may be due to reasons related to the unawareness and training among organization's employees as well as the weakness of the applied control tools and procedures (Anwar, 2017, 15:16).

Given the increasing importance of information technology in governmental organizations and the public sector, many audits conducted by SAIs' auditors should consider information technology issues and include related components.

As a result, the field of electronic information systems auditing, known as information technology auditing and information security auditing, emerged to address the challenges facing organizations with the endless developments in information technology in order to avoid and eliminate any risks that

information systems might be exposed to as well as to ensure that the possibility of their systems being exposed to any internal or external threats has become detectable.

Therefore, the researcher addressed the topic of the conceptual framework for electronic information systems auditing as follows:

Section One: Auditing Information and Communication Technology

Section Two: Electronic Information Systems Risks

Section One
Auditing Information and Communication Technology

1/1/1 Preamble

The global nature of information technology has changed the method we all work with in various ways, and the auditing profession is no exception. As technology advances, businesses, governments and public sector organizations adopted information technology in their information systems aiming to increase efficiency and enhance the delivery of their various products and services. The pattern of deliverying public services has also rapidly shifted from physical to electronic. This shift has forced governmental organizations to act as digital platforms for delivering services to the public, in addition to providers of the IT infrastructure that supports them. The ongoing digital transformation of information has also led to an increased general reliance on IT systems (Rabii, 2023, 539: 551).

As the audited organizations increase their investment in and reliance on IT systems, it is essential for the IT auditor to adopt an appropriate methodology and approach. This can help ensure that the audit is able to identify the risks threatening data integrity, availability, validity, misuse and privacy as well as how to address those risks and vulnerabilities (Hussein, 2020, 25: 50).

1/1/2 The concept of auditing Information and Communication Technology (ICT) systems

An ICT audit could be generally defined as an examination of the aspects of an organization's use of information technology, including information technology infrastructure, controls, policies, procedures, applications and data use. It is the process of collecting and evaluating evidence to determine whether the use of computers contributes to protecting the organization's

assets, ensuring its data integrity, achieving its objectives effectively and using its resources efficiently (Younis and Mustafa, 2015, 104).

ICT audit is also known as the audit whose subject deals with the organization's information technology systems, their management, operations and all related procedures and processes, or as the audit that examines information and communication technology systems to ensure that they meet the organization's needs without compromising important characteristics of the organization, such as security, privacy and cost (INTOSAI, 2023, 9).

Such an audit might be entirely dedicated to information technology issues, or it might be part of a targeted audit towards a specific topic. In both cases, the goal of the technological audit is to identify deviations from specific standards that have been identified based on the type of audit, such as a Financial Audit, Compliance Audit or Performance Audit.

1/1/3 Requirements for conducting IT audits

The mandate of the Supreme Audit Institution to conduct IT audits is stipulated in Lima Declaration (INTOSAI, 1977). Also, the SAI mandate to conduct IT audits is derived from the general mandate of SAIs to conduct Performance, Financial and Compliance Audits or a combination of both, in accordance with the Fundamental Principles for Public Sector Auditing (INTOSAI, 100:2019), the Principles for Financial Auditing (INTOSAI, 200:2020), the Principles for Performance Auditing (INTOSAI, 300:2019) and the Principles for Compliance Auditing (INTOSAI, 400:2019).

1/1/4 Scope of ICT Auditing

ICT auditing works in conjunction with different types of auditing, as the ICT auditor's activity may intersect with the work of the financial auditor through his examination of the financial statements and auditing operations by evaluating the audit in the organization's various activities. It intersects with Performance Auditing in evaluating aspects related to ICT, and is consistent with special purpose auditing when it is related to evaluating services provided by a third

party. It can also intersect with Forensic Auditing and Compliance Auditing (INTOSAI, IDI, 2022, 10), for example:

- In the context of Financial Auditing, an example of an IT audit could be the examination of the general controls that ensure the information systems' operation that underlie the SAI's financial operations, as shown by its financial statements (INTOSAI, 200, 2020) .
- In the context of Performance Auditing, an example of an IT audit could be determining the extent to which the SAI's adoption of new technology has led to measurable benefits at the government level and cost savings (INTOSAI, 300, 2020).
- In the context of Compliance Auditing, an example of an IT audit could be the examination of the effectiveness of information systems that produce compliance reports, enabling employees to manage and control the SAI's operations. This could include, among other things, analyzing the audited entity's compliance with GDPR requirements or IT-related legal actions (INTOSAI, 400, 2020).
- An IT audit may not be part of a Performance Audit, a Financial Audit, or a Compliance Audit; however, the general principles, procedures, standards and expectations applicable to Financial, Performance, and Compliance Audits also apply to IT audits.

  IT audits may address a variety of diverse areas, such as IT governance, IT investments, whether there are adequate data protection controls for entities such as local governments, analyzing the implementation of new technologies such as artificial intelligence, or the development, acquisition and operation of IT systems. They also address aspects of information security and cybersecurity, to which they are closely related (ISACA, 2019, 23: 45).

  Since an IT audit is an examination of controls, these controls are represented in any procedures to reduce the risk of harmful events. They might be manual or automated procedures, a policy, a method, a practice,

a process, etc. Controls could be classified as General Controls and Special Application Controls (INTOSAI, 2019, Standard 5100).

A- General Controls: These aim to achieve the desired characteristics of information (e.g., confidentiality, integrity, availability) in the human, technical, financial, physical and other environments in which information systems are developed, maintained and operated.

B- Special Application Controls: These are manual or automated procedures that rely on information technology within an information system that affect information processing. Special Application Controls could deal with data verification, processing, communication, security and related issues.

These Controls are discussed in detail in the second section of this chapter.

1/1/5 Types of ICT Audits

Types of ICT audits can be identified as follows (Richard, 2015, 9:15) :

1. Media and Communication Strategy Audit

It is an audit that aims to ensure that the information system is consistent with the organization's general strategy, specific challenges and risks. It is not enough for the information system to be compliant with the laws and controlling them, but it should also be aligned with the organization's regulations and culture; and that investments directed to information technology serve the current and future needs of the organization.

2. Media and Communication Function Audit

It is an audit that aims to ensure that the organizational structure and operations are aligning and consistent with the rules, whether the operations are related to planning, direction, application development and providing services and support.

It is worth noting that the primary reference for this type of audit is the Control Objectives for Information and Related Technology (COBIT) publications.

3. Auditing the organization's computerized operations

This type of audit aims to ensure that the information technology system is secure and that the system's operation is secure, continuous and safe, as these characteristics are considered conditions for business continuity in the organization, and should be taken care of given that malfunctions, data loss and threats resulting from open networks increase possible risks in the organization. In this context, the audit is concerned with everything related to the system being secure - system availability, service continuity, reliability, security and maintenance - and the availability of these characteristics currently and in the future in the organization.

It is also possible to differentiate between the following types: (Abu Al-Haija, 2017, 50: 55) (Abu Shaiba, 2017, 80: 98)

1- Auditing around the computer

In this type of audit, the auditor completely ignores the computer, and runs a group of operations manually from beginning to end by obtaining their original documents, then compares his/her outputs with the outputs of the organization's electronic operation.

2- Computer-based auditing

This type of auditing includes examining and testing the automated and situational control procedures of the automated system to verify their adequacy and safety. There are several methods for this type of auditing:

-The auditor could prepare a set of mock operations similar to the organization's actual operations and operate them using the organization's devices and programs, in order to evaluate the situational control procedures that go into designing the organization's programs.

-The control programs method: which requires the auditor to prepare programs similar to the organization's programs and operate the organization's actual operations and compare the results, in order to test the ability of the organization's programs to produce accurate data and to ensure that the organization's data cannot be modified.

-The general audit programs method: the general audit programs are programs capable of performing some audit procedures. One of the most important operations of these programs is parallel simulation which involves using the same main files, the same operations files, producing the same outputs and comparing the outputs of the simulation process with the actual outputs.

3- Computer auditing

Its procedures include auditing the data operation process inside the computer and auditing the inputs and outputs where the auditor verifies the validity of the inputs, the operation process and the outputs' validity.

1/1/6 Characteristics of the ICT Systems Audit Environment

The ICT systems audit environment is distinguished by a set of characteristics that could be summarized as follows:

First: Internal Control and Rrisk Assessment

1- Internal control in the ICT environment

Internal control in the ICT environment is characterized by including a set of manual procedures and others designed in computer programs. The importance of internal control of ICT systems increases due to the multiplicity of risks between the disappearance of physical records and the disappearance of the audit document, as well as the risks of fraud and damage resulting from viruses, in addition to the risks resulting from the inefficiency and negligence of employees (Al-Tayeb and Al-Siddiq, 2014, 144) (Al-Saadawi, 2017, 32: 38).

Internal control within the framework of ICT systems is characterized by the following:

(IFAC, ISA 315, 2013) (Alsaleem & Husin, 2023, 1: 24)

A. The internal control system contains manual and automated elements, and the characteristics of these elements affect the risk assessment and the quality of procedures followed.

B. The organization can use automated procedures to directly record, process, and report on transactions, and in this case electronic records replace paper records.

C. The organization's use of manual and automated control procedures varies according to the type of organization and the degree of its reliance on information technology. Each of these two types has its own risks, as automated procedures result in risks of unauthorized access, unauthorized changes in programs and systems as well as damage to data and systems. They are characterized by ensuring the consistency of pre-determined procedures and rules, ensuring the flow of information and increasing the ability to implement the separation of duties through security and control elements in applications, databases and operating systems.

D. General control programs on information technology are represented by policies and procedures related to applications and support the effective work of their controlling elements as well as maintain the integrity of information and data security. These programs can be preventive to guard against errors, or exploratory to identify the occurring risks.

E. Relying on automated systems to operate data leads to the integration of many manual processes into one step, which leads to weak control resulting from the separation of tasks, and imposes an increase and tightening of audit procedures to control risks well (Al-Wardat, 2019, 260).

2- Risks in the ICT environment

ICT systems produce more risks, which are: (Al-Wardat, 2019, 262) (Dallal and Al-Fattal, 2019, 23:30)

A. Business application risks: which result from the soundness and integrity of data exchanged between different parties, especially since these parties are often not known to each other.

B. Process integration risks: which indicate the user's exposure to the risks of changing or losing data, its duplication during implementation and incorrect operation of data as a result of weak control procedures; i.e. risks resulting

from changing data when changing or modifying other files as a result of weak control.

C. Information protection risks: These risks result from violating the confidentiality of data exchanged using the Internet.

The researcher discussed these risks in detail in the second section related to the risks of electronic information systems.

3- Risk assessment stages in the ICT environment

The stages and methods of risk assessment in ICT systems can be considered as rings including different levels of control, where if the current level fails to prevent the error, it moves to the next level. These levels are as follows: (Hussein, 2020, 1: 72)

A. Risk prevention stage: The main audit goal at this level is to avoid the occurrence of the error.

B. Risk detection stage: In this stage, the goal is to design methods for monitoring potential risks and reporting them to officials.

C. Reduction of risks' impacts stage: When the risk occurs, the goal is to reduce the losses resulting from it to the greatest extent possible. An example of this is the organization's keeping backup files of the main files to reduce the losses resulting from the risk of the original files' damage.

D. Investigation and verification stage: In this stage, investigations are carried out to find out the cause of the risk in order to provide useful information in developing a security policy related to the systems.

Second: Documentation

Documentation is the recording of the implemented audit procedures, the appropriate evidence obtained and the conclusions reached. The International Auditing Standards stipulate that the auditor should document his/her work by documenting his/her mission plan and audit program, the nature, extent and timing of carrying out his/her tasks, the characteristics on the basis of which he/she selects the elements that will be examined, determining the results of the procedures for examining these elements as well as the various problems

and issues of importance related to the elements that were examined and the findings reached during the audit process (2009 230, IFAC, ISA).

The advantage of documentation appears in the ICT environment due to the disappearance or scarcity of documents and paper evidence leading to the disappearance of the audit trail and the absence of evidence that clarifies the operations' implemenation stages. The trail of operations' processing becomes within the system hence intangible, especially if the documents are present and the input is done in one place,while the inputs are processed and the outputs are obtained in another place (Al-Dhiba, et al. 2014, 34).

On the other hand, documents in Information and Communication Technology systems are divided into: (Suleiman, 2017, 70: 75) (Manish, et al., 2018, 20: 25)

1- The complete main documents file: It represents the papers related to the system from the orders for establishing work teams, written programs and their logical diagrams, ending with matters related to the application, the most important of which is the system application message.

2- The operating instructions file: It is a file prepared by the programmers who wrote the system programs, each according to the programs they contributed to, and it is delivered to the operations department's official for following it up.

3- The punching instructions file: It is a file prepared by the system designer and programmers and consists of punching and audit instructions for all inputs as well as punching and audit programs for each input type.

4- Audit file: This file is prepared by the system designer and programmers, and it includes the instructions that the control department should follow during the operational cycle, starting from receiving and recording inputs, returning rejected inputs, tracking their receipt with corrections and delivering outputs to the appropriate officials at the appropriate time.

5- Beneficiaries file: This is prepared by the system designer and basically includes how to fill out the input forms, the cases and times in which they

are submitted to the computer department, in addition to various audit procedures such as auditing samples of outputs and other procedures that are important to the proper functioning of the system and its effective operation.

1/1/7 Objectives of ICT Systems Audit

The objectives of ICT systems audit do not differ from the general objectives of auditing, but this type of audit is distinguished by its contribution to achieving a set of specific objectives and goals that revolve mainly around assessing the extent to which ICT contributes to serving the organization's objectives.

The primary objective of ICT systems' auditing is to provide adequate protection for the organization's assets, and these assets vary between: (Chris, 2015, 32: 35)

- Data of various types in its broad sense and its related documentation systems and others.
- Manual and electronic operating systems.
- The technology used in the organization, including equipment, operations systems, database management systems, communication systems and multimedia used in performing operations and in communication.
- Individuals and their possessed skills, awareness and productivity that enable them to plan, program, acquire, transfer, support and monitor information systems and related services.

In general, the audit of Information and Communication Technology systems aims to achieve a set of objectives, which are: (Bradford, M., et al, 2020, 521: 547)

A. Economy: This objective is represented by the auditor's endeavour to examine the computer's use in order to ensure that the technology is used to the maximum possible capacity to serve the organization and at the lowest possible costs. These required information and data are provided at the appropriate time, which benefits the institution.

B. Effectiveness: The auditor's goal is to examine the effectiveness of the audit tools to ensure the efficiency of the internal control system in all activities as well as administrative, financial and operational functions.

C. Adequacy: The auditor should verify the use of technology to meet the most important requirements for the institution, according to the Relative Importance Principle.

D. Protection: This objective means that the auditor ensures that the Information and Communication Technology system is protected from various risks associated with its use, such as system collapse, loss of data stored on disks, virus problems, data damage and theft, or deliberate sabotage that systems may be exposed to to cover violations that may be committed by some employees.

The objectives of auditing Information and Communication Technology systems can also be determined through the auditor's field of interest as follows: (Krasna, 2017, 20: 25) (Al-Zaza, 2016, 15: 17)

A. Application: This objective means that the auditor ensures the existence of audit controls to provide reasonable assurance that the organization's operations are complete, correct and recorded in an appropriate manner and time.

B. Development: The audit of Information and Communication Technology systems aims to contribute to the systems' development before and after their implementation, to ensure that they contain appropriate audit controls, and to ensure that the organization's interests are met and integrated into the system.

C. Operational processes: This objective includes paying attention to the audit environment and addressing any deficiency or weakness in the general control systems to avoid negative impacts on various activities and institution functions.

D. Management: This objective focuses on assessing the inclusive audit environment and organizing information systems in addition to assessing the

weaknesses that may affect various applications, especially with regard to the administrative aspect.

E. Technology: The aim of auditing Information and Communication Technology systems is to audit a specific technology used in the system, for the purpose of a general assessment of the audit environment.

1/1/8 The importance of auditing Information and Communication Technology systems

The importance of auditing ICT systems is evident through the increasing role of the auditor in the organization as a result of the integration of technology into the institution's various activities and departments, which added a new role to the auditor as a result of the electronic operation of most of the data and transactions that will be operated. It has become necessary for the auditor to be familiar with the systems in place and to participate in its design to evaluate the system and know its strengths and vulnerabilities in addition to being familiar with the types of risks resulting from technology.

The importance of auditing ITC systems is also evident through its necessity to understand the ICT elements and components. It is an important mechanism that works to create value for technology in the organization, reduce the risks resulting from it, acknowledge the various aspects related to technology in the organization, measure the maturity of technology in the organization and allow management to know the extent to which practices related to ICT in the organization are consistent with internationally recognized standards and frameworks (Abu Sheiba and Al-Futtaimi, 2017, 1: 20).

The importance of auditing ICT systems is increasing due to the large spending of institutions on technical aspects, which increases their need to ensure systems' consistency and their security against various threats and attacks (Al-Dhaiba et al., 223; 225) (Karso', 2023, 30: 49) (Slapnicar, 2022, 1: 21).

1/1/9 Tasks of the Information and Communication Systems' Auditor

The IT systems auditor performs a number of tasks, the most important of which are: (289, 2013, Alan & Taljanovic)

A. Evaluating the internal control systems on the inputs in terms of their preparation and entry into the system as well as the programs used in operation and processing.

B. Ensuring the integrity and validity of the programs used in processing inputs and their suitability to achieve the system's objectives. He/she may seek the assistance of experts and specialists in this regard.

C. Ensuring the validity of the equipment for electronic data operation in terms of operational integrity.

D. Ensuring the integrity of the methods and means of analyzing data using the computer and that they fulfill the desired purpose.

E. Ensuring the soundness of the protection systems of programs and devices used in the system's operation, the regularity of maintenance operations on a regular basis, as well as the regularity and continuity of the updating and development operations to ensure the efficiency and effectiveness of the system's outputs.

F. Ensuring the integrity and accuracy of the information distribution system, its protection and retrieval capabilities as well as ensuring the effectiveness of the feedback system.

g. Ensuring the integrity of the files to protect them from any possible manipulation.

h. Ensuring that modifications made to electronic data operating programs are approved by a party with the appropriate authority and authorization, and that these modifications are objective and consistent with the latest developments in the internal and external environments.

10/1/1 Legal frameworks, standards and guides for auditing information and communication technology systems

The Lima Declaration (INTOSAI 1977) provides the general basis for the legal framework governing IT audits by Supreme Audit Institutions. It states that the establishment of Supreme Audit Institutions should be defined in the constitution and details may be specified in legislation, and in paragraph 22 of the Lima Declaration, the mandate for audits of electronic data processing facilities is presented with the main aspects of these audits. There may also be specific mandates for Supreme Audit Institutions to conduct IT audits. These frameworks also include national laws on information security or privacy, information security strategies, etc.

The audit of information and communication technology systems is subject to generally accepted standards in all types of auditing, but the characteristics of the regulatory environment for this type of audit, and the distinction of the evidence and its procedural aspect, obliged international organizations interested in auditing in general to develop a general framework for the profession by issuing a set of standards and guidelines specific to the nature of this field. (Taherdoost, 2022, 1:20)

IT audit standards and guides play a crucial role in guiding auditors and directing their efforts. They provide a unified framework and internationally accepted standards for conducting audits efficiently and effectively.

As a reliable reference, standards and guides also contribute to standardizing practices and enhancing communication between auditors and stakeholders, which enhances transparency and confidence in audit results and the resulting recommendations.

International standards and frameworks relevant to IT audits include guidance issued by the International Organization of Supreme Audit Institutions (INTOSAI), such as INTOSAI 5100:2019 on the Audit of Information Systems, as well as the WGITA IDI Handbook on IT Auditing for Supreme Audit Institutions (WGITA – IDI 2022).

The WGITA IDI Handbook covers IT auditing, IT governance, development and acquisition, operations, outsourcing, business continuity planning, disaster recovery planning, information security, application controls and additional important topics.

The frameworks also include the Information Systems Performance Assessment Handbook issued by the EUROSAI Information Technology Group in 2024.

ISACA has provided important frameworks and guides on IT audits. The Technology Audit Framework, ITAF, 4th Edition (ISACA 2019) provides standards for information system audits and, in its previous editions, guides on information system audits, information system audit tools and techniques and assurance. ISACA has published several editions of the COBIT framework for governance and management of information and technology. These frameworks should be considered in conjunction with other guidance on SAIs and their audit levels, such as the Fundamental Principles for Public Sector Auditing (ISSAI 100). Legislation on financial and performance auditing also helps to understand the technological inclusion and the need for IT audit skills. For example, the Fundamental Principles for Financial Auditing (ISSAI 200), the Principles for Performance Auditing (ISSAI 300), and the Principles for Compliance Auditing (ISSAI 400) complement each other. Other important standards and guidance include:

A. International Federation of Accountants Publications

The Federation, through its subsidiary (IAASB) "International Auditing and Assurance Standards Board", issued a set of standards and statements as follows:

- International Standard on Auditing (ISA 401) "Auditing in a Computer-Based Information Systems Environment"

-International Standard (ISA 315) (Revised) entitled: "Identifying and Assessing the Risks of Material Misstatement through Understanding the Organization and Its Environment"

-International Standard (ISA 400) Risk Assessment and Internal Control

-Standard (ISA 330) "The Auditor's Response to Assessed Risks"

B. Statements of the International Committee of the Auditing Profession:

This committee has issued four basic standards:

-Statement 1001: Computerized Information Systems Environment - Stand-alone Personal Computers

-Statement 1002: Computerized Information Systems Environment - Live Computer Systems

-Statement 1003: Computerized Information Systems Environment - Database Systems

-Statement 1008: Risk Assessment and Internal Control Characteristics and Considerations for Computerized Information Systems

-Statement 1009: Computerized Audit Methods

c. International Organization for Standardization (ISO) Publications

The International Organization for Standardization (ISO) is an international organization that issues standards that provide global specifications for products, services and systems to ensure quality, safety and efficiency (Al-Sarna, 2021, 251: 260) (Alan & Steve, 2013, 65: 75). This organization has developed many standards related to IT auditing, including:

-ISO9000: Quality Systems

-ISO31000: Risk Management

-ISO38500: IT Governance

-ISO27002 / ISO 27000 / ISO 27001 for Information Security

-ISO 27006 for the requirements of the entity providing the audit

-ISO 27007 Guidelines for Auditing Information Security Management Systems

-ISO 27008 Guidelines for Auditors on Information Security Management Systems Controls

D. Publications related to project management, internal control and governance

-Issuance of the PMBOK Guide, the practical guide For project management.

-COSO version of internal control. (IIA IPPF, 2017)

-IT governance framework for control objectives of information and related technology (COBIT). (ISACA, 2019, 20: 25)

At the European level, EUROSAI has published audit reports and surveys that may assist in the implementation of IT audits in various areas. One of the objectives of the EUROSAI European IT Working Group is to assist European audit bodies in their IT audits.

The European Agency for Information Security (ENISA) has also published guidelines and studies that may be relevant to IT audits. (EUROSAI ITWG, 2023)

At the Arab level, the Arab Organization, through the Information Technology Oversight Committee, concluded a memorandum of cooperation with the EUROSAI Information Technology Working Group to exchange knowledge, expertise and joint projects in the field of information technology audits, in addition to holding a scientific symposium on information technology on the sidelines of the third meeting of the Information Technology Oversight Committee held in Tunisia in October 2023, and the Arab Organization holding a scientific conference on modern methods of information systems oversight, which was hosted by the Central Auditing Organization in Cairo in July 2024.

11/1/1 Information and Communication Technology Systems Auditing Path

Before starting the audit, the auditor must take into consideration preparing the process of selecting the core axes of the auditing process, understanding the

organization's information environment and adapting to it, understanding and analyzing data within the framework of the law, and taking into consideration information retrieval and alerting to software risks. (Friday, 2019, 29: 30)

Figure No. (3) illustrates the IT auditing path

Source: Prepared by the researcher

The general path for auditing information and communication technology systems includes a set of steps that appear as follows:

First: Planning and risk assessment

IT audit planning is considered the most important stage, as this step determines the general path of the audit process, and ensures that the task is carried out with high quality, in an economical, effective and efficient manner, and in line with the organization's objectives. It is a crucial stage that establishes a successful assessment of the organization's IT infrastructure, processes and controls.

IT systems audit planning includes strategic auditing, which is a long-term planning set by the supreme audit body in the country, comprehensive planning, which is plans carried out by the auditor for the audit operations he performs during the year, and partial auditing, which is planning for each operation separately.

The following is an overview of the planning process, types of planning, risk assessment, and the concept of risk-based auditing. (INTOSAI WGITA, IDI, 2022, 9: 14)

A. Types of Planning

The planning process includes the following types: (Mohammed, 2017, 58: 65)

1- Initial Planning

-**Objectives Determination**: Determine the purpose of the audit, including understanding the business objectives and specific objectives of the IT audit.

-**Scope Determination**: Determine the limits of the audit, including identifying the systems, processes and departments that will be audited.

-**Resource Allocation**: Allocate the necessary resources, including audit team members and the tools and techniques required for the audit.

2- Detailed Planning

-**Risk Assessment**: Conduct a detailed risk assessment to determine priorities.

-**Audit Program Development**: Create an organized plan that outlines audit procedures, timelines and key milestones.

-**Information Gathering**: Collect relevant documents, such as IT policies, procedures, previous audit reports, meeting minutes, regulatory requirements, describe the technical status of the organization and various developments therein, review contracts related to the use of third-party services.

3- Communication Planning

-**Stakeholder Engagement**: Identify key parties and inform them of the audit plan, objectives and expectations.

-**Meeting Coordination**: Schedule meetings with stakeholders to discuss the audit plan and address any concerns.

B. Risk Assessment

Risk assessment is an important part of the IT audit planning process, which involves identifying potential threats to the IT environment and assessing their potential impact and likelihood of occurrence, including the following: (INTOSAI WGITA, IDI, 2022, 9: 14) (Balqasem, and Hussein, 2017, 25: 55)

1. **Risk Identification**: Identify risks related to IT systems, such as data breaches, system failures, and non-compliance with systems.

2. **Impact and Likelihood Assessment**: Assess the potential impact of each risk on the organization's operations and the likelihood of its occurrence.
3. **Prioritization**: Categorize risks based on their impact and assess their likelihood to focus on the most significant threats.
4. **Mitigation Strategies**: Identify controls and strategies in place to mitigate these risks.

C. Risk-Based Audit

The risk-based audit approach focuses on prioritizing audit activities based on the level of risk. This approach ensures that audit resources are allocated to areas of greatest importance, including: (Hassan, 2017, 30: 35)

1. **Risk assessment**: Conducting a comprehensive risk assessment to identify and assess risks.
2. **Audit planning**: Developing an audit plan based on identified risks, with a focus on high-risk areas.
3. **Control evaluation**: Evaluating the effectiveness of existing controls in mitigating identified risks.
4. **Audit procedures**: Designing audit procedures that target high-risk areas, to ensure a thorough examination of critical controls and processes.
5. **Reporting**: Providing detailed findings and recommendations, with a focus on areas where risks were not adequately managed.

A. Audit Design

Audit design can be considered part of the IT audit planning phase. It involves developing a structured approach to how the audit will be conducted. This overlaps with all previous planning procedures, and the following elements typically fall within the audit design at the planning phase (INTOSAI WGITA, IDI, 2022, 14: 17)

1. **Define objectives**: Clearly state what the audit seeks to achieve.

2. **Define scope**: Identify areas, systems and processes to be examined, based on need and in accordance with the initial audits performed. The scope of the audit includes control systems related to the use and protection of information and communication technology resources in their broad sense, which includes data, operating systems, technology, licenses, people and IT governance; and other IT-related matters.
3. **Risk assessment**: Assess potential risks to prioritize focus areas.
4. **Develop methodology**: Establish methods and procedures that will be used to collect and analyze data.
5. **Allocate resources**: Identify the people, tools and technologies required for the audit.
6. **Define timeline and milestones**: Define a timeline with deadlines and milestones.
7. **Establishing an audit program**: Formulating a detailed audit program that specifies the steps and procedures for conducting the audit.

Effective IT audit planning includes comprehensive preliminary and detailed planning, a comprehensive risk assessment, adopting a risk-based audit approach, and by focusing on high-risk areas and ensuring strong communication with stakeholders. This ensures that the audit is designed to be systematic, comprehensive, organized, effective, and consistent with the organization's objectives and risks, and protects its technological and information assets.

Second: Implementing the audit process

Implementing the audit process goes through a set of basic stages represented by collecting evidence, inspections and field visits to end with the initial report and then the final report. These stages include procedures for examining and evaluating the internal control system and collecting more detailed data and information to identify important weaknesses that the auditor focuses on in his tests.

These steps can be explained as follows: (INTOSAI, WGITA, IDI, 2022, 18:22) (Al-Bari, 2023, 45: 55) (Abu Amr, 2023, 31: 35) (Juma, 2019, 30: 35)

A. Collecting audit evidence

The auditor collects evidence before the field visit stage of the institution, and this stage includes an in-depth examination of the policies and procedures related to the areas identified in the scope of the audit to be audited, including documents related to data protection policies, the practical guide for procedures related to sensitive data, data protection training models, risk registers, information asset registers, information governance structure, etc.

This procedure aims to ensure that the next stage, which is the field visit, will be effective by identifying the people who will be interviewed and the processes that will be examined;

B. Field Visit

This phase usually takes two to three days of the assignment time, and the field visit begins with a meeting with the board members in order to explain the audit process to them and to discuss the problems and issues related to the audit and answer the questions they have about the IT systems audit process.

During this phase, several procedures are carried out to obtain evidence, which are multiple between:

1. **Initial assessment of IT controls**: This includes general controls and application controls to derive an understanding to confirm that they are reliable and sufficient to achieve the audit objective.

2. **Objective tests**: Based on the assessment of controls, auditors may identify priority areas for objective tests, which include detailed tests of controls.

3. **Physical examination:** This means the inventory or actual examination carried out by the auditor on the tangible assets of the institution;

4. **Confirmations:** This means collecting evidence from a source other than the organization being audited, which is known as the third party, to which the auditor sends the information he wants to verify, so that this party can confirm or deny it;
5. **Verification:** This means examining the organization's documents and papers;
6. **Analytical procedures:** Analytical procedures consist of making comparisons and relationships to determine the logic of a piece of information;
7. **Inquiry from the client:** This means obtaining information from the client, and the client means the organization being examined. In this context, the organization's website or e-mail can be used to obtain this information as a means of saving time and cost;
8. **Restart:** This means that the auditor restarts part of the system to judge the efficiency of the system's operation and the effectiveness of the control procedures.
9. **Audit documentation:** This is a record of the audit work carried out and the evidence supporting the results and conclusions, and it must comply with the requirements of reliability, completeness, sufficiency and accuracy.

The researcher believes that going through the previous stages enables the auditor to identify the basic problems in the organization's information and communication technology systems.

Third: Audit and Reporting Report

The reporting stage is considered one of the most important stages of IT auditing, as it concludes the audit efforts and presents the results and recommendations to stakeholders and concerned parties. The report

represents the final product of the audit process, and is a tool for communicating and reporting the audit results. This reporting must include the results of the audit mission, its objectives, the scope of the audit process, and the results reached. These results must be communicated accurately, objectively, clearly, unified, constructively, and completely, and must be issued in a timely manner.

Given the specificity of the audit of information and communication technology systems, the IT systems auditor's report must contain: (INTOSAI WGITA, IDI, 2022, 23:25)

A. Audit scope statement: The auditor must accurately determine what are the main axes and areas that were examined and included in the audit process. It can also clarify what areas were not included in the mission, and this paragraph helps overcome misunderstandings;

B. Executive Summary of the Audit Process: The ICT auditor must write an executive summary that includes a detailed listing of the issues addressed and an explanation of the work plans. The summary of the issues means highlighting the issues of significance or relative importance compared to others. This summary must be:

- Expressive of the task so that those who do not have time to read all the details can rely on it and understand the task in general, including the control procedures and the work environment based on the summary;
- Serve as an informational document for the reader even if it is separated from the rest of the report;
- Includes information related to the audit results in general;

C. List of issues and work plans: This list is the basic element of the report, as it includes details about the important issues that were discovered and the measures taken to resolve them. This element must be understandable so that it provides an appropriate understanding for individuals dealing with the audited area of the audited issues, and provides the Board of Directors with information about the risks and the reasons for the need to mitigate them;

D. Additional items (optional): There are some additional items that are not essential in the report, but there may be a need to list them in the report, and this relates to:

- Basic control controls: If the auditor notices some control controls that are important in the area or field that was audited, he can include them in the report with the problem that was addressed, in order to encourage good procedures and comment on inappropriate controls in order to draw the attention of officials to improve them;
- Closed items: If the organization resolves some issues during the audit period, these items are considered closed, meaning that they have been addressed, and in this case they must be referred to in the report in appreciation of the organization's proactive efforts, and to ensure that the report gives a complete picture of the problems at the time of its presentation;
- Simple issues: The ICT auditor may find some issues or problems that are simple, or do not pose a major risk, and therefore there is no need to develop plans for them or issue decisions regarding them, but the auditor can include them in the report by way of drawing attention to them, and as a way of informing managers about them and leaving the decision to them.

Preparing the initial report does not mean publishing it directly, as the auditor allows the organization to review the initial report with the possibility of commenting on it before it is issued. After preparing and reviewing the initial report, the final report can be issued and submitted to the Board of Directors, or to the Board and the Audit Committee, as the case may be.

Fourth: Follow-up

The follow-up stage is a vital and essential part of the success of the IT audit process, as it ensures that the recommendations presented in the audit report are effectively implemented and any issues identified are appropriately addressed. This stage helps close the audit process cycle and ensures continuous improvement in the organization's IT controls and operations, and

that the organization maintains a strong and effective control environment. (INTOSAI WGITA, IDI, 2022, 23)

12/1/1 The impact of information and communication technology systems on audit procedures

According to the international statements 1001 and 1002 for auditing, the computer environment affects the audit procedures as follows:

A. The computer environment makes it difficult and expensive to provide adequate controls, so the auditor assumes that the control risk is high in this case. In this case, when assessing the risks, the auditor must plan to reduce detection errors since the control risk is high. (Karsoo, 2023, 30: 49)

B. It is appropriate for the auditor in this case to, after obtaining an understanding of the control environment and the flow of transactions, focus on substantive tests near or at the end of the financial year, which requires increasing physical examination and confirmations of assets, as well as increasing detailed tests and expanding the sample size, and using computer-based audit methods whenever possible and appropriate;

C. Computer-based audit methods may include the auditor using his own software, and he may use the organization's software and compare the results of information processing, and the auditor may develop a special audit method;

D. The control procedures that the auditor takes into consideration include: (Taha et al., 2016, 271: 284) (Ali and Shahata, 2015, 15: 27) (Manish et al., 2018, 43: 45)

1) Segregation of duties and balance controls: This includes separating and rotating tasks among employees, in addition to management reviewing reports and tables that identify the employees using the system and the tasks assigned to them;

2) Access to the computer and files: This includes placing the computer within sight of the person responsible for monitoring it to facilitate his access to it, using keys to lock the computer and sub-devices, using passwords to restrict

access to programs and data files, and placing restrictions on public benefit programs. Audit Statement 1002 states that data access controls aim to detect and prevent any unauthorized access, change, or use of data and programs;

3) Use of third-party software: When an organization purchases software from a third party, it must examine these programs before purchasing them, and ensure their functions, capacity and controls, and appropriate selection of software and modifications to them before use, and continuous evaluation of the software must be carried out to ensure that it meets customer requirements;

4) Providing controls for developing and maintaining systems: This includes procedures to ensure that the necessary controls for direct applications, such as passwords, access controls, direct data validation and restart procedures, have been included in the system during its development and maintenance;

5) Providing programming controls: These include procedures designed to prevent or detect inappropriate changes to computer programs, which have been accessed through direct sub-devices. In this context, access to programs should be restricted and all changes to programs should be documented;

E. There are some applied controls in ICT systems, which are:

1) Prior authorization for processing: such as using a bank card with a personal identification number before making a cash withdrawal through the machine;

2) Periodic auditing of system inputs and processing results: to ensure the completeness, accuracy and reasonableness of evidence and processed data;

3) Cut-off procedures: procedures to ensure that transactions have been processed in the appropriate accounting period;

4) File controls: special procedures to ensure that correct data files are used in direct processing;

5) Master file controls: since the importance of the master file imposes more stringent procedures than the rest of the files and processing;

6) Balancing: a procedure to create control groups on the data divided for processing through direct sub-devices, and compare control groups during and after processing, to ensure complete and accurate data transfer, for each stage of processing.

13/1/1 IT Audit Tools and Techniques

IT auditors generally use a variety of tools, techniques and programs to audit IT in the entities subject to their supervision, including for example: (Ghanimi, 2017, 420: 490) (Chris & others, 2015, 99: 120)

1. Vulnerability scanning tools: used to analyze network infrastructure and systems to identify potential security vulnerabilities.
2. Penetration testing tools: used to test the security of systems and applications by simulating real attacks to identify security vulnerabilities and provide recommendations for correcting them.
3. Safety and security monitoring tools: used to monitor unauthorized activities and compliance with security policies and legal directives.
4. Protection management systems: manage and monitor security and protection by analyzing policies and reports and providing recommendations for improvement.
5. Incident management and security response systems: used to deal with, investigate and respond to security incidents effectively.

6. Access control and identity verification systems: used to manage access to data and resources securely and efficiently.

7. Log analysis and monitoring tools: used to monitor and analyze activity logs to detect abnormal or suspicious patterns.

The researcher believes that these tools and techniques used vary based on the specific audit needs and security requirements of each entity.

1/1/1 IT Audit Areas

The IT audit process includes a wide range of areas that aim to evaluate the effectiveness, efficiency and controls of an organization's IT systems. Here are some of the basic audit areas:

(INTOSAI WGITA, IDI, 2022, 26: 95) (Pandzo &Taljanovic, 2013, 288: 294)

(Alwardat, 2019, 65, 70) (Al-Bari, 2023, 20: 28) (Al-Zaza, 2016, 220: 230)

A. Information Security and Cybersecurity

Information security refers to a set of measures and procedures that aim to protect information from potential threats and risks, whether they are of an actual nature such as breaches and leaks, or of an intangible nature such as human and natural errors. It aims to ensure the integrity and confidentiality of information, the integrity of systems, and to provide appropriate access to authorized users only.

While cybersecurity refers to a specific branch of information security that focuses specifically on protecting digital systems and networks from cyber attacks, which may include hacking, malware, phishing, and other online attacks.

In general, cybersecurity is a part of information security, focusing on protecting digital infrastructure and systems from cyber threats, while information security

includes all aspects related to maintaining the integrity and confidentiality of information in general.

Information security auditing and cybersecurity auditing can be part of an IT audit, where the systems and technologies used to protect digital information, data, and systems are evaluated in a broader context.

An IT audit focuses on evaluating and auditing all aspects of technology used in an organization, including hardware, software, networks, database systems, storage, etc. Among the aspects of technology that are audited, information security and cybersecurity can be an important part.

B. System Operations Audit

A system operations audit focuses on evaluating the efficiency and effectiveness of the operational processes of information systems. This includes verifying:

- System performance: ensuring that systems operate efficiently and meet user needs.
- Incident management: assessing how incidents, technical problems, and emergency responses are handled.
- Backup and recovery management: verifying the existence and sustainability of backup and data recovery procedures.
- Security: examining the security controls in place to protect data and information from unauthorized access.

C. IT governance audit

IT governance audit focuses on evaluating the policies and procedures that govern the use and management of information technology within the organization. This includes:

-Governance structure: assessing the governance structure of information technology and ensuring that it is aligned with the organization's objectives.

-Risk management: examining the processes used to identify, assess, and manage IT risks.

-Compliance: ensuring that the organization complies with relevant IT regulations, laws, and standards.

-Accountability and transparency: assessing the clarity of roles and responsibilities related to information technology within the organization.

D. IT investment audit

IT investment audit aims to evaluate how resources and investments in information technology are managed to ensure that the desired return is achieved. This includes:

-Cost-benefit analysis: Verifying that IT investments are made after conducting comprehensive cost-benefit analyses.

-Project management: Evaluating project management processes to ensure that they are implemented within the specified timeline and budget.

-Strategic planning: Examining the extent to which IT investments are aligned with the organization's overall strategy.

-Performance monitoring: Ensuring that there are mechanisms in place to monitor and evaluate the performance of IT investments to ensure that the specified objectives are achieved.

e. IT systems maintenance audit

The aim of IT systems maintenance audit is to evaluate the processes and procedures related to the maintenance and updating of information systems. This includes:

-Change management: Evaluating the processes used to manage system changes and ensuring that they follow recognized practices.

-Update and upgrade procedures: Verifying that updates and upgrades are carried out in a systematic and safe manner.

-Technical support and maintenance: Examining how technical support and maintenance are provided to systems and ensuring their efficiency.

-Documentation: Ensuring that all maintenance processes are properly documented and up-to-date.

Auditing various IT areas, including information security and cybersecurity, plays a critical role in enhancing the security, efficiency and effectiveness of IT systems, thus supporting the achievement of an organization's goals

15/1/1 The role of supreme audit institutions in the field of IT audit

The role of supreme audit institutions in the field of IT audit is represented in several aspects, the most important of which are the following:

(EUROSAI ITWG, 2023, Training course) (INTOSAI WGITA, IDI, 1: 9)

1. Setting policies and guidelines: Supreme audit institutions play an important role in setting policies and guidelines related to IT auditing in government organizations. This role is to define security standards and requirements and guide institutions on how to implement them effectively.
2. Review and evaluation: Supreme audit institutions review and evaluate the performance of government organizations in the areas of IT auditing, including assessing the extent of compliance with security policies and standards and the effectiveness of the security measures in place.

3. Directing reforms and improvements: Based on the results of the evaluations and reviews, supreme audit institutions direct the necessary reforms and improvements in the areas of security auditing in government institutions, with the aim of enhancing cybersecurity and protecting the state's vital data and systems.
4. Guidance and technical support: Supreme Audit Institutions provide guidance and technical support to government institutions in the areas of IT auditing, including providing advice and technical guidance to implement best practices and adopt the latest security technologies.
5. Security awareness and education: Supreme Audit Institutions play an important role in spreading security awareness and education about the importance of security auditing and combating cyber threats, with the aim of enhancing the security culture within government institutions and enhancing their ability to address security threats.
6. Coordination between government agencies: Supreme Audit Institutions play an important role in enhancing coordination between the various government agencies concerned with cyber security, which contributes to achieving comprehensiveness and reducing cyber vulnerabilities and threats.

The researcher believes that Supreme Audit Institutions play a vital role in ensuring information security, maintaining the stability of government systems, and enhancing their ability to address increasing cyber threats. These agencies need continuous updating and close cooperation with government institutions and the private sector to make the most of their efforts in this regard.

The researcher believes that to enhance the capabilities of the supreme audit institutions in the field of IT auditing, the following can be followed:

1. Enhancing specialization and technical competence: Appropriate training and professional development must be provided to employees in the

supreme audit institutions to enhance their knowledge and skills in the fields of IT auditing, information security and cybersecurity.

2. Using advanced technologies: The necessary resources must be provided to adopt and use modern technologies and big analysis tools to enhance the effectiveness of auditing and monitoring operations.
3. Providing continuous professional training and development: To enhance the professional capabilities of auditors in the field of IT auditing and information security and to benefit from modern technology in the field of auditing.
4. Enhancing partnerships and cooperation: Cooperation must be enhanced with other government agencies, academic institutions, professional organizations, peer bodies and the private sector to exchange knowledge and expertise and develop joint solutions to enhance cybersecurity.
5. Improving infrastructure and resources: The necessary resources, whether technological or human infrastructure, must be provided to enable the supreme audit institutions to perform their duties effectively.
6. Exchange of expertise and knowledge: By participating in teams, working groups and committees concerned with IT auditing, big data and the impact of science and technology on auditing within the INTOSAI community.
7. Develop policies and standards: IT auditing policies and standards must be developed and updated periodically to ensure that they keep pace with technological developments and cyber threats.
8. Promote security awareness and education: Society and organizations must be made aware of the importance of cybersecurity and how to address cyber threats through ongoing educational and awareness campaigns.
9. Develop monitoring and analysis capabilities: The capabilities of supreme audit institutions in the areas of monitoring and analysis must be developed to enable them to effectively detect and confront cyber threats.

10. Provide ongoing guidance and support: Government organizations must be provided with ongoing guidance and support in the areas of IT auditing, information security and cybersecurity by supreme audit institutions.

11. Promote transparency and accountability: Work must be done to promote transparency and accountability in auditing and oversight processes to ensure integrity of work and its compliance with legal and security standards and requirements.

The researcher believes that by adopting these steps and focusing on continuous development and joint cooperation, supreme audit institutions can effectively enhance their capabilities in the field of IT auditing.

16/1/1 Experiences of Supreme Audit Institutions in IT Audit

In this section, we discuss some practical cases of IT audits by Supreme Audit Institutions as follows: (EUROSAI ITWG, 2023, IT audit training course)

1. **Audit of the Supreme Audit Institution in Germany on the digital transformation of administration in 2023**

The German e-Access Act requires public administration in Germany to provide most of its services digitally by the end of 2022. The Ministry of the Interior is the coordinator of the spread of digital technology in public administration.

The audit of the Supreme Audit Institution in Germany on the digital transformation of administration indicates that the Ministry has prepared two programs to implement the e-Access Act. One program was dedicated to administrative services provided at the federal level and another program to administrative services provided jointly by federal, state and local governments. An amount of 3.5 billion euros was allocated to implement the e-Access Act. By the end of 2022, about 52% of these funds had not been used and 19% of administrative services that could be implemented digitally were available online.

The audit notes that the Department spent almost half of the statutory implementation period defining which administrative services should be digitalised, as well as the extent and order of these services. Technical specifications, requirements and key IT solutions were delayed, resulting in duplicate and multiple developments.

The audit recommends, among other things, that the Department should better coordinate the implementation of the eAccess Act and ensure that technical specifications and requirements are available in a timely manner. Centralised IT solutions should help avoid simultaneous development. The Federal Government needs to work towards a federal government digital and technology strategy.

2. The UK Supreme Audit Institution's 2023 audit of government services transformation

The UK Auditor General's 2023 report addressed the obstacles to effective digital transformation in government. It notes that in 2021, Cabinet established the Central Digital Data Office (CDDO) to lead the digital and data function across government. In 2022, the Central Digital Data Office published the Digital Data Roadmap for 2022–2025, which highlights six cross-government tasks, including the task of creating transformed public services that deliver the required outcomes. According to this task, at least 50 of the top 75 government services listed in the Roadmap Annex should be moved to the "excellent" standard. The "excellent" standard requires that services reduce unnecessary time, effort and cost for both their users and the departments that provide them. According to the initial analysis conducted by the Central Digital Data Office, 10% of the services listed in the Roadmap had reached this standard at the time of publishing the SAI's report. As of 2023, the Central Digital Data Office was working to understand how efficiently the 75 services listed in the strategy were operating and to establish a baseline for the performance of all these services, with a focus on

measuring performance for the main users of these services. As part of the set of functional standards to guide UK government workers, the Central Digital Data Office has developed Government Functional Standard GovS 005: Digital, which focuses on the management of services, technology and data, as well as digital governance practices.

The report recommends, among other things, that the Central Digital Data Office keep the scope of the roadmap activities under constant review to ensure they are aligned with available resources, with prioritisation where needed.

3. Australian SAI audit of supply chain security risks in 2022

In 2022, Australia's SAI investigated how three government entities, the Australian Federal Police, the Australian Taxation Office and the Department of Foreign Affairs and Trade, comply with established supplier security requirements.

The report explained that Australian government organisations rely on supply chains of organisations, people, activities, information and other resources to deliver digital services and to keep them secure. To deliver these services, they must implement the Preventive Security Policy Framework (PSPF) as Australian government policy. It includes principles, findings and sixteen policies, including Policy 6, which deals with security governance for contracted providers of goods and services.

In the above report, contracts were selected for each audited entity to support the assessment of compliance with the requirements of Policy 6. The auditors found, among other things, that the contracted suppliers had implemented many, but not all, of the processes and controls in accordance with the PSPF.

For example, one contract provider, Telstra Australia, had implemented security measures to restrict administrative privileges for certain specified network devices. However, Telstra had not implemented patches for operating systems on network devices in accordance with the PSPF

requirements and Hitachi Vantara, another contract provider, had implemented patch management processes for operating systems and applications, but the Australian Federal Police had not implemented patch management processes for applications on Hitachi servers.

None of the audited entities identified terms and conditions relating to non-compliance management in relation to the PSPF and the entity's internal policy requirements.

The audit recommended, among other things, that the audited entities should implement processes to verify the reliability of performance information and non-compliance management of contract providers against the PSPF and the Australian Cyber Security Centre's Information Security Manual, as well as the entity's internal policy requirements. The three entities agreed with this recommendation.

4. The Supreme Audit Institution of the Netherlands' 2020 cybersecurity audit

The Supreme Audit Institution's cybersecurity audit of the border controls at Amsterdam Airport included controls operated by the Dutch Border Guard. The audit focused on three technical systems that support the pre-screening of arriving passengers, the checks carried out at passport offices, and the checks carried out at the self-service passport gates at Amsterdam Airport Schiphol. The Minister of Defence was responsible for the cybersecurity of the first two systems, and the Minister of Justice and Security was responsible for the security of the third system.

According to the audit, the Ministry of Defence's security policy requires annual security tests, but this requirement was not actually followed. The auditors arranged a test of the IT system used for the pre-screening in November 2019.

This test revealed eleven vulnerabilities, including the use of standard passwords, the possibility of sending fake emails in the name of Ministry of Defence officials, and the use of outdated software. These vulnerabilities could

allow a DoD employee with access to the DoD network but not authorized to access the pre-screening system to infiltrate the system and manipulate its operations. The audit report notes that DoD took steps to prevent such an attack.

In 2018, DoD hired a contractor to conduct a security analysis of the self-service system, however, the audit concluded that this analysis did not reveal any critical risks.

In 2018, DoD commissioned one of its departments, the Defense Computer Emergency Response Team (DefCERT), to conduct security testing of the self-service passport gate system. This testing identified one vulnerability classified as “high risk” and seven vulnerabilities classified as “moderate risk.” DefCERT concluded that additional testing was needed to make recommendations on the overall health of the self-service system project. The vulnerabilities found in this testing were removed following the audit. The auditors recommended, among other things, that the Minister of Defence and the Minister of Justice and Security conduct annual security tests of the three IT systems used in border controls and ensure that the recommendations resulting from the tests are implemented.

The Minister of Defence and the Minister of Justice and Security responded that the fourteen critical systems of the Ministry of Defence would be required to pass a security test and implement measures based on its recommendations every three years. The annual testing of the self-service system was planned to begin in 2021.

17/1/1Common observations in IT audits

The most common observations found when auditing electronic information systems, and the risks associated with them, can be classified as follows: (EUROSAI ITWG, 2023, IT training course) (Gantz, 2014, 50:60)

A. Observations related to security and access

1. Passwords are not changed regularly, which can lead to unauthorised access to data and resources.
2. Lack of monitoring logs of user movements, which hinders the detection of unusual activities and potential security incidents.
3. Using weak or short passwords or not applying password complexity policies, which increases the risk of unauthorized access.
4. Not implementing multi-factor security measures to enhance protection against unauthorized access.
5. Not defining access levels, which can increase the system's exposure to hacking risks.

B- Notes related to user management

1. Lack of periodic reviews of user privileges, which can lead to inappropriate privileges and security breach risks.
2. Not training users on security practices, which contributes to increasing hacking risks.
3. Delaying the disabling of user accounts after they leave work or reach retirement age, which increases the risk of unauthorized access.
4. Not clearly defining user responsibilities, which leads to overlapping privileges and increased security risks.

C- Notes related to technical infrastructure

1. Using unsupported systems, programs and devices, which leads to compatibility and security issues.
2. Untested updates to programs and applications, which can cause security and stability issues.
3. Failure to implement and test regular backup procedures, which may lead to data loss in the event of a disaster.
4. Using outdated and outdated devices, which gives attackers the opportunity to take advantage of known vulnerabilities.

5. Failure to provide regular training to employees responsible for the technical infrastructure, which leads to incorrect decisions regarding security and maintenance.

D- Notes related to records and monitoring

1. Failure to activate control controls in data centers and the absence of visitor records can lead to weak physical security, lack of accurate records of user movements.
2. Delay in reviewing and analyzing security records can cause unusual events not to be detected in a timely manner.
3. Using ineffective monitoring systems can lead to missing important events in the monitoring process.
4. Lack of clear policies and procedures for monitoring security and responding to security incidents can increase the risk of data loss and hacking.

D- Notes related to financial data

1. Incomplete ledger in the electronic system, and entering and processing transactions outside the information system.
2. Differences in serial numbers for entering transactions in the electronic information system.
3. Errors in entering daily transaction data, for example, errors in entering foreign exchange rates.
4. Financial transfers to some suppliers without corresponding purchases in the information system.

R- Notes on strategic planning and spending on information technology

1. Time pressure or unrealistic schedule leading to delays in delivery and implementation of untested systems while ignoring or postponing information security.
2. Neglecting information security requirements during the concept and design phase, neglecting information security vulnerabilities leading to disruptions and delays in fixing information security vulnerabilities

3. Poor coordination between IT and business stakeholders leading to increased project costs due to inefficiency
4. Lack of a multi-year strategic IT plan. Without a long-term plan, IT investments are not aligned with business objectives, leading to overspending and suboptimal resource allocation.

18/1/1 Challenges Facing IT Auditing

IT auditing faces several challenges related to resources, technologies, and rapid developments in the field of technology, some of which are as follows: (Karsoo, 2024, 30: 49) (Engel, 2024, 265; 290) (Hernan, 2019,240: 250) (Davis, 2021, 230: 260)

1. Evolution of cyber threats and attacks: With the increasing sophistication of cyber threats and the emergence of new offensive techniques, it is difficult for audit teams to keep up with all potential vulnerabilities in systems and networks.
2. Technical complexity: The complexity of digital infrastructures and information systems increases with the development of technology, making security analysis and auditing more difficult and complex.
3. Lack of specialized human resources: The lack of expertise and skills in the field of cybersecurity and technology auditing represents a challenge, as it is difficult to find qualified personnel to implement operations efficiently.
4. Time pressure and scheduling: Determining audit schedules and completing them on time is a challenge, especially given the urgent need to maintain the security of data and systems.
5. Compliance with standards and regulations: With the increasing restrictions on legal compliance and security legislation, ensuring compliance with these standards and regulations becomes an additional challenge for audits.

6. Dealing with large volumes of data: The challenges of IT auditing also include dealing with large volumes of data and analyzing them effectively to detect vulnerabilities and threats.
7. Integration of technologies and systems: The complexities of integration between different technologies and information systems can make security verification more complex.
8. Legal challenges and international legislation: Changes in international laws and legislation may require a new perspective on auditing processes, which adds additional challenges to organizations.

The researcher believes that these challenges require clear strategies and strong cooperation between different departments within the organization, in addition to investing in the technologies and tools necessary to deal with them effectively.

19/1/1 Confronting the challenges facing IT auditing

The researcher believes that to overcome the challenges facing IT auditing operations, multiple strategies can be followed, including the following:

1. Enhancing the professional capabilities of auditors: This is done by encouraging them to obtain professional certificates in the field of IT auditing, such as the Certified IT Auditor certificate, as well as participating in working groups and committees concerned with IT auditing in the INTOSAI, EUROSAI and ARABOSAI communities, as well as participating in initiatives issued by international and professional organizations to enhance the skills of auditors in general and IT auditors in particular, such as obtaining the IT Audit Certificate for Non-IT Auditors issued by the EUROSAI organization during 2023, as well as attending scientific and training meetings in the field of IT auditing, for example the scientific meeting organized by the ARABOSAI organization entitled Modern Methods of Controlling Information Systems during July 2024.

2. Awareness and training of employees: Security awareness and training of employees is vital to confronting cyber threats, and training can include topics such as identifying cyber attacks and how to confront them and cybersecurity practices.
3. Use advanced technologies: Using advanced technologies such as artificial intelligence and big data analysis in audits can increase the efficiency and effectiveness of security verification processes.
4. Simplify processes and procedures: Simplifying security processes and procedures can facilitate the audit process, reduce human errors, and increase compliance with policies and regulations.
5. Improve transparency and communication: Strengthening internal and external communication and enhancing transparency in security processes can facilitate audits and contribute to better achieving their objectives.
6. Enhance cooperation and coordination: Encouraging cooperation and coordination between different departments within the organization and with external parties can enhance the effectiveness of audits and better direct efforts.
7. Adopt a culture of compliance and responsibility: Encouraging a culture of compliance with security policies and individual responsibility for cybersecurity can enhance security awareness and reduce the risk of breaches.
8. Invest in continuous modernization and development: Investing in continuous modernization and development of security systems and technologies can help address evolving cyber threats and improve the organization's ability to adapt to changes.

The researcher also believes that implementing these strategies effectively can contribute to enhancing information security and ensuring that audits fully meet the specified objectives.

Section Two
Electronic Information Systems Risks

1/2/1 Introduction

In our current era, electronic information systems have become a fundamental building block in the infrastructure of most organizations and societies, and these complex systems are a vital platform for storing, processing and transferring data and information. With the increasing electronic exchange of information, the importance of securing and protecting these systems increases significantly.

Given the importance of the government institutions sector and the important role it plays in the process of economic, social and administrative development, by providing data that contributes to preparing plans, budgets and decisions that contribute to solving problems in light of the challenges they face from environmental and political conditions surrounding them, and the technological progress witnessed by this sector in terms of developments that led to the transformation of manual work procedures into automated ones, these organizations have relied on information technology systems. (Daifallah, 2017, 201: 220)

Electronic information systems face a variety of risks, ranging from simple cyber threats such as malware and viruses, to more sophisticated threats such as offensive hacks and hybrid hacks. These risks also vary to include hacks by internal hackers, threats related to fraud and data theft, and even geopolitical threats that include international cyber attacks. It is important to realize that these risks are not limited to large systems only, but also extend to individuals and families, especially with the increasing use of Internet-connected devices in our daily lives. Securing electronic information systems requires serious attention and continuous efforts from all concerned parties,

and these efforts must include effective strategies to prevent cyber attacks and enhance security awareness.

1/2/2 The concept of electronic information systems

An electronic information system can be defined as a system that aims to manage and organize information electronically in all fields. An electronic information system includes the use of technology to store, enter, retrieve, process, and transmit data effectively and in a timely manner.

It also refers to the systems and technologies used to collect, store, process and transmit information electronically. These systems include a variety of software and technological infrastructure that support the exchange of information between users and systems. (Al-Ghabour, et al., 2019, 360: 408) (Al-Fatlawi, 2021, 25: 27)

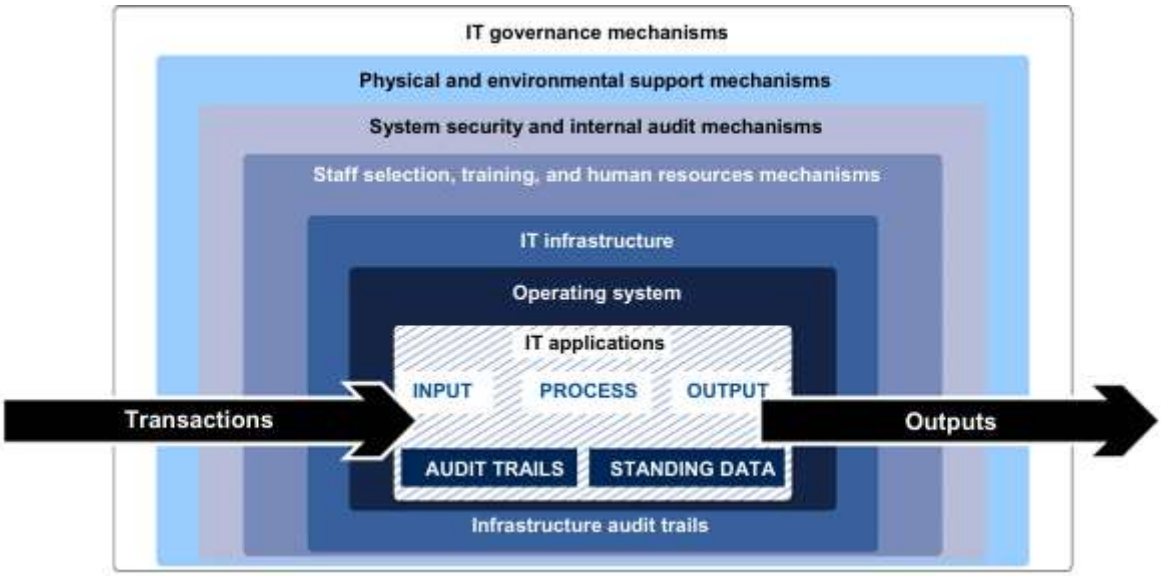
Electronic information systems include many elements, the most important of which are:

(Maddah, 2021, 20: 25) (Al-Marri, 2023, 1303, 1373) (Aburman, 2021, 32: 30)

1. Software: Includes content management software, customer relationship management systems, data storage systems, and security and protection software, which are used to manage and process information effectively.
2. Hardware: Includes servers, storage devices, network devices, and end devices (such as computers, tablets, and smartphones), which work together to enable the operation and management of electronic systems.
3. Networks: Provide the necessary infrastructure to connect devices and exchange information between them, whether they are internal local networks or wide-area networks via the Internet.
4. Storage and database technologies: Used to store data securely and efficiently, and allow quick access to information and manage it in an organized manner.

5. Communication and exchange technologies: Include technologies that enable the exchange of information between users, such as email, chat, social platforms, and document sharing systems.
6. Security and protection management systems: Used to protect data and information from security threats, and include technologies to protect against viruses, malware, and cyber-attacks.

Figure No. (4) illustrates the electronic information system



Source: INTOSAI IT Audit Initiative Guide, 2022

1/2/3 Objectives of Electronic Information Systems

Electronic information systems aim to achieve a variety of objectives that contribute to improving the organization's performance and enhancing the effectiveness of internal and external operations. The main objectives of electronic information systems are as follows: (Al-Mutairi, 2023, 1: 27) (Al-Naqbi and Al-Masabi, 2023, 1815: 1907) (Ali and Shahata, 2015, 10: 15)

1. Improving access to information: The electronic information system aims to provide quick and easy access to important and necessary information for employees, management, customers and partners.

2. Increasing the efficiency of operations: The electronic information system simplifies daily operations and improves their organization, which contributes to increasing work efficiency and reducing the time and effort expended.
3. Improving communication and cooperation: The electronic information system contributes to enhancing communication between the organization's various departments and its employees, and facilitates cooperation and the exchange of information and resources between members.
4. Providing support for decision-making: The electronic information system contributes to analyzing data and generating reports and statistics that help in making better and more accurate strategic and tactical decisions.
5. Improving customer service: By providing quick access to information about products and services and processing customer requests effectively, the electronic information system contributes to improving customer satisfaction and strengthening relationships with them.
6. Improving resource management: The electronic information system helps in better managing financial, human and material resources, which contributes to reducing costs and increasing efficiency.
7. Increasing competitiveness: The electronic information system aims to enhance the competitiveness of the organization by improving processes and providing new opportunities for innovation and development.
8. Improving the quality of products and services: The electronic information system can contribute to monitoring and improving the quality of products and services by monitoring processes and collecting and analyzing feedback.
9. Increasing employee satisfaction: By providing advanced technical tools and resources, the electronic information system can increase employee satisfaction and improve the work environment.
10. Improving security and confidentiality: The electronic information system seeks to protect sensitive information and ensure data confidentiality by implementing security, encryption and access control procedures.

11. Improving relations with partners and suppliers: The electronic information system can facilitate communication and exchange of information with partners and suppliers, which enhances cooperation and contributes to improving business relations.

These are some of the main objectives of electronic information systems, and they can be customized according to the needs and goals of each institution or organization.

1/2/4 Characteristics of electronic information systems

In order for management to be able to fulfill its responsibilities and achieve the goals it seeks, the necessary information must be provided in quality, time and cost, and this is done through information systems. There are many features that make electronic information systems able to achieve the desired goals effectively. The following are some of the main characteristics of electronic information systems: (Al-Mutairi, 2023, 1: 27) (Aburman, 2021, 30)

1. Data storage: Electronic information systems are characterized by the ability to store large amounts of data in a secure and organized manner.
2. Ease of access: Electronic information systems provide easy means of accessing data and information, whether through graphical user interfaces or effective search systems.
3. Information sharing: Electronic information systems enable the sharing of data and information between different departments and individuals within the organization.
4. Providing security and confidentiality: Electronic information systems ensure the implementation of appropriate security measures to protect data and ensure the confidentiality of sensitive information.
5. Integration: Electronic information systems allow integration with other systems within the organization such as customer relationship management systems and human resource management systems.

6. Analysis and reporting: Electronic information systems allow the analysis of data and the creation of reports and statistics that support decision-making processes.
7. Flexibility and expansion: Electronic information systems are characterized by flexibility and the ability to expand to keep pace with the changing needs of the organization.
8. Coordination and organization: Electronic information systems help in coordinating and organizing processes and data effectively to improve work efficiency. There is no single system that is suitable for application in all organizations because, although the system has a similar general structure, the internal components differ from one facility to another.

Despite these characteristics, however:

- The information system should not remain rigid in its application in a single organization and should be modified whenever necessary.
- The use of electronic information systems should be evaluated from time to time to explore the strengths to generalize them and the weaknesses to avoid them.
- Feedback in information systems is also the basic element to ensure its continued effective application.

1/2/5 The role of electronic information systems in decision-making and taking

Electronic information systems play a vital role in the decision-making process in institutions, as they provide the data and information necessary to make informed and evidence-based strategic and tactical decisions, as follows: (Al-Naqbi and Al-Masabi, 2023, 1815: 1907) (Aburman, 2021, 20: 25)

1. Providing data and information: Electronic information systems collect, store and organize data and information from various sources within the institution, making it easier for decision-makers to access the necessary information.
2. Analysis and evaluation: Electronic information systems enable the comprehensive and accurate analysis of data and information, which helps in understanding the current situation and evaluating available options.

3 .Generating reports and statistics: Electronic information systems enable the generation of reports and statistics related to specific information, making it easier for decision-makers to extract important results and information.

4 .Supporting decision-making processes: Electronic information systems provide the necessary support to decision-makers by providing the data and analysis necessary to make sound and evidence-based decisions.

5 .Forecasting and planning: Electronic information systems help in predicting future trends and developing appropriate plans and strategies to deal with them.

6 .Communication and coordination: Electronic information systems contribute to improving communication and coordination between different members of the organization, which facilitates the process of exchanging information and making joint decisions.

The researcher believes that electronic information systems work to support the decision-making process by providing data, analysis and communication between different departments, which helps in making effective and fact-based decisions.

1/2/6 Electronic accounting information systems

Accounting information systems are an essential part of electronic information systems in organizations. These systems aim to organize, process and present accounting and financial information in an effective and accurate manner, and to meet the organization's needs in the field of financial reporting, money management and financial data analysis. The following are some of the main aspects of accounting information systems as part of electronic information systems: (Qardash and Qansouh, 2023, 1: 21) (Al-Munizel, 2022, 36: 40) (Abu Al-Haija, 2017, 25: 27)

1 .Recording financial transactions: Accounting information systems record and document all financial transactions that take place in the organization, such as purchases, sales, payments and entitlements.

2 .Preparing financial reports: Accounting information systems enable the preparation of the necessary financial reports for the organization, such as income statements, balance sheets, cash flow statements, budgets and final accounts, accurately and on time.

3 .Account Management: Accounting information systems enable the effective management of financial accounts, budgets and financial statements, making it easier for management to make sound financial decisions.

4 .Analytical Reports: Accounting information systems help analyze financial data and prepare analytical reports that contribute to understanding the organization's performance and identifying future trends and directions.

5 .Tax Compliance and Assessment: Accounting information systems adhere to tax and accounting compliance standards, and help prepare the necessary reports for tax assessment and compliance with applicable financial laws and regulations.

6 .Internal Control: Accounting information systems provide mechanisms for internal control and ensuring the accuracy and integrity of financial information, through the application of appropriate accounting policies and procedures.

The researcher believes that accounting information systems are a vital part of electronic information systems, and contribute to managing financial information and providing the necessary data to make sound financial decisions and ensure compliance with accounting and tax standards.

1/2/7 Types of risks facing electronic information systems

Information technology risks are defined as anything that results in an error or malfunction in information technology that leads to a negative impact on the organization's business and its information systems.

In this context, electronic information system security risks can be classified and classified from different perspectives as follows: (Abu Shaiba, Al-Futtaimi, 2017, 80: 98) (Al-Jarbou, 2023, 1363: 1430)

A- In terms of their source

-**Internal risks**: Organization employees are considered the main source of internal risks to which electronic information systems are exposed, because they are aware of the system information and are more familiar than others with the applied control system and its strengths and weaknesses in the organization, and they have the ability to deal with information and access it through the access powers granted to them, and therefore, untrustworthy organization employees can access data and potentially destroy, distort or modify it.

-**External risks**: Information hackers and natural disasters are the most important sources of external risks. Information hackers usually exploit their high skills in computers and information technology to illegally enter systems and programs with the aim of manipulating or destroying data or for the purpose of theft and embezzlement. They may try to penetrate regulatory and security controls with the aim of obtaining confidential information about the organization, while some natural disasters such as earthquakes,

volcanoes and floods may result in partial or total destruction of the system in the organization.

B- In terms of the cause

-**Risks resulting from the human element**, which may be the result of some unintentional human actions (as a result of error or oversight) or intentional with the intent to deceive and manipulate.

-**Risks resulting from the non-human element**, in which humans have no role and which are the result of natural disasters related to power outages and fires.

C- In terms of intentionality

-**Risks resulting from deliberate actions**: These risks are considered to be very influential risks on the system, such as the deliberate entry of incorrect data or the deliberate destruction of data in some important files or parts thereof, usually by deleting, modifying or distorting data in some records and files or creating misleading or incorrect information in order to hide the effects of fraud and manipulation and theft of some money or some important data.

-**Risks resulting from spontaneous and unintentional actions**: These are actions carried out by people as a result of ignorance and lack of sufficient experience, such as entering data incorrectly due to their lack of knowledge of how to enter it or oversight or error, and these risks can most often be corrected or avoided with more training for employees and good supervision over them.

D- In terms of the resulting effects

-Risks that result in material damage to the system and computer devices or the physical destruction of data storage media, which may result from some natural phenomena such as floods, earthquakes, power outages or fires, or from the collapse of systems or networks for certain periods.

-Technical or logical risks: which may affect the data in the computer memory or on magnetic tapes, and this may be by distorting programs and

introducing computer viruses that may negatively affect the availability of data when needed, by withholding it from persons authorized to view or use it or disclosing confidential data to persons not authorized to view it, which may affect the integrity of data and programs within the system.

E- In terms of its relationship to the stages of the system

-**Input risks**: The risks related to the security of the inputs are represented in creating false data - modifying or distorting the input data by manipulating the inputs and original documents after they are approved by the official and before entering them into the system - deleting some inputs before entering them into the computer - repeating the data entry more than once.

-**Data operation risks**: The impact of these risks is on the data stored in the computer memory and the programs that operate this data. The risks of data operation are represented in modifying and distorting programs - making illegal copies of programs - using the program in an unauthorized or unlicensed manner - introducing time bombs and viruses into computers - distorting and modifying programs using a Trojan horse or other methods that require specialized expertise in computers and programming.

-**Output risks**: These are the risks related to the information and reports obtained after the operation process. The risks of computer outputs are represented in stealing computer outputs, obliterating or destroying certain items of the outputs, creating false and incorrect outputs, misusing them, making unauthorized copies of the outputs, or directing them to persons who are not authorized to receive or view them due to their confidentiality or because they are not authorized to view them and do not have the security requirements, in addition to creating false data.

Risks related to electronic information systems can be classified as follows (Hussein, 2020, 20:50):

A) Risks related to information technology infrastructure, which are as follows:

1- Inadequate encryption of data and information.

2- Inadequate procedures for preventing theft and illegal access to information.

3- Absence or lack of integrity of support and assistance procedures.

4- Confronting physical risks such as fires.

5- Absence of backup procedures.

B) Risks related to information technology applications, which include:

1- Inadequate software security procedures related to the security of the information technology infrastructure.

2- Inadequate controls for entering and extracting data.

3- Malfunctions or errors in information technology applications.

4- Unauthorized changes in the programs used.

C) Risks related to e-commerce:

The American Institute of Certified Public Accountants indicates that the risks of e-commerce are due to the following reasons (Davis, 2021, 25:30) (Gantiz, 2014, 35:50):

1- Deliberate attacks: These occur by hackers or competitors of the organization with the aim of accessing the company's confidential information, such as customer credit card numbers, confidential information related to customers, sales volume, and many things that may be difficult to enumerate.

2- Privacy of dealings: Electronic dealings that take place between individuals and the company are of a very important informational nature, because they are stored in the digital memory of the system, and they are very valuable information that someone may be able to know or even track and hack, and thus the customer will lose confidence in the company he dealt with on the basis that it was unable to protect his privacy.

3- Loss of trust: This means the organization losing trust in its client's information. It is well known that the client uses what is called his

digital signature to enter the organization's system in order to complete his desired transaction, so what if the wrong person was able to enter using the client's signature.

4- Failure of the transfer process: Although the electronic purchasing process is done very quickly, it exposes him to the risk of failure of the transfer process. It is well known that the purchase process via e-commerce is done through several steps. The consumer begins by filling out the initial form and other steps that may be necessary according to the company's policies. At each stage, a new page is opened on the organization's website, and for technical or other reasons, one of the steps may fail, and here a new problem will appear, which is the lack of certainty that the process has been completed.

5- Lack of documentation: In traditional trade, the transaction is usually documented with supporting papers drawn with the organization's logo and signed by the appropriate person, and through personal and direct contact between the seller and the buyer, but all of these matters are almost completely missing in e-commerce, and this fact increases the likelihood of dealing with the wrong person.

6- Identity theft: In the absence of proper documentation as in traditional commerce, it has become easy for criminals to impersonate others and carry out operations without their knowledge.

7- Falsification of facts: The services of some marketers and security service providers will be cosmetic services only in the absence of a specific mechanism that confirms their credibility and the effectiveness of their services.

8- Effects of economic pressures: The rapid growth of e-commerce has led to it becoming a competitive market, and the real strength of the competitor lies in the success of the security and reliability mechanisms

related to its accounting system, as whoever can provide these mechanisms has a greater share in this global technological market.

d) Risks related to hacking that occurs via the Internet

The reasons for the difficulty of tracking hacking that occurs via the Internet are as follows:

1- Speed of the process, the intruder (hacker) may not need more than a few minutes to hack a specific site, manipulate it and leave the site before being tracked.

2- Lack of a specific identity, it is not possible to know who the hacker is, in any way.

3- Distances, the hacker may be thousands of kilometers away in another country, as the Internet is designed globally.

4- The ability to access from several places, as the online user does not need a specific place to access the network, as anyone can access the network from anywhere where there is a computer and a communication line, such as Internet cafes, university laboratories and schools.

5- The absence of international laws, as the Internet is a global network with unified standards for use only, and if we assume that a hacker is discovered in a country other than the country of the organization that was hacked, it is not necessary to have unified laws to deal with the hacker.

6- The ability to destroy computer data If any hacker feels that he can be tracked, he can destroy his device with the simple push of a button, which makes the process of tracking him useless and useless.

1/2/8 Reasons for the risks facing electronic information systems

The components of the electronic information system (individuals, procedures, data, programs, information technology infrastructure, internal control, information security requirements) are exposed to risks for any of the following reasons: (Khalil and Ibrahim, 2014) (Abu Rumman, 2021, 30: 35) (Al-Munizel, 2021, 40: 45)

1 -Increasing individuals' experience in using computers and knowing the weaknesses in the system through which it can be hacked by the organization's employees.

2 -Lack of adequate protection against the risks of viruses and hacking.

3 -Failure to define responsibilities and powers for each individual within the organizational structure, and failure to separate tasks and functions related to the organization's information systems.

4 -Lack of specific policies and programs for the security of information systems in the organization.

5 -Failure to apply the principles and standards of information security governance

6 -Weakness and inefficiency of the control systems applied to detect these risks if they occur.

7 -Some of the organization's employees share the same passwords to access the system.

8 -Technological progress and rapid software development in the computer industry.

1/2/9 The extent to which the modern business environment needs preventive measures for electronic information systems

The absence of appropriate controls and procedures allows opportunities for manipulation and sabotage in electronic information systems by irresponsible persons from inside or outside the company.

In general, the IT auditor is required to test controls related to technology, and at a minimum, all auditors must understand the control environment of the organization subject to audit in order to provide assurances regarding the internal

controls operating in the organization. According to the basic principles of the International Standards of Supreme Audit Institutions for Public Sector Audit, auditors must obtain an understanding of the nature of the entity, department or program to be audited, including an understanding of internal controls, in addition to the objectives, operations, organizational environment, systems and business processes involved.

Control procedures (components of an effective internal control system) under electronic information systems are represented in three main groups: (Al-Munizel, 2021, 23:25) (Al-Wahib, 2022, 36:51)

1 -General control procedures.

2 -Control procedures on applications.

3 -Control procedures on the database

The following is a brief presentation of these procedures:

1 -General control procedures:

These are the procedures related to all or most of the applications that are done by computer and these procedures are related to controlling the following:

A- Separation of functions:

The functions in the electronic data processing department and the functions in the departments using information must be separated, and the importance of this separation increases in the case of functions related to each of:

1 .Authorization powers

2 .Implementation and registration

3 .Preservation of assets

4 .Accounting responsibility

The electronic processing department should be responsible only for the registration function and the other functions are the responsibilities of other departments within the organization.

B- Authorities to authorize and approve the development, purchase, and change of software before using it in data processing:

These authorities include the following:

1. The departments using the information must participate in designing the systems alongside the electronic processing department.
2. Employees of the departments using the information must participate with the employees of the electronic processing department in testing the new systems.
3. The approval of the organization's management, the departments using the information, and the electronic processing department must be obtained to introduce the new systems before starting to use those systems.
4. Control must be tightened over the transfer or copying of the main file or some of the operation files in order to prevent unauthorized changes to their contents and to ensure the accuracy of the results when using those files.
5. Programs and systems must be well documented as well as the changes that occur in them.
6. Proposals for changes submitted by the departments using the information or submitted by the electronic processing department must be documented.
7. The director of the information systems department must study and evaluate all changes made to the programs and systems.
8. Programs that are modified must be tested using test data.
9. Programs that are being run must be compared with saved copies of those programs in order to detect any unauthorized changes in those programs.

A- Access permissions to data files:

These permissions include the following:

1. Access permission to programs, data files and computer devices must be limited to persons authorized to deal with them, such as operating employees, their supervisors and others who are permitted to access devices, programs and data.
2. Access to the computer room must be controlled to prevent unauthorized persons from entering it.
3. A record must be kept of visitors who visit the computer room after being authorized to do so and accompanied by an authorized person.

4. A personal code or password must be used to limit access to programs to authorized persons.
5. Use the call system to identify and distinguish persons authorized to access the computer system.
6. Data must be encrypted when stored in files or when transferred from old locations to the computer system via networks or otherwise.
7. Grant program operators' free access to operating manuals containing processing instructions while concealing program details from them.
8. The monitoring team must monitor operators' activities and schedule their work.

B- General control procedures built into the system itself

There are general control procedures built into the computer system and these procedures give the computer the utmost confidence from those who use it. This confidence is mainly due to the progress and development of chip technology. The procedures built into the computer system are self-diagnostic means to detect and prevent hardware failures. The following is a review of some of these procedures:

- Diagnostic devices and programs: These are devices and programs provided by computer manufacturers with these computers to be used in examining operations and electronic processing methods within the computer system.
- Operating range protection: In most central processing units, several operations are performed simultaneously. In order to ensure that the operations that are being performed simultaneously will not interfere with each other (causing damage or change), the programs contain procedures to protect the range of each operating process.

C- Other general control procedures

There are other general control procedures, which are as follows:

1 .Using a backup file retention system to retrieve data in the event of damage, to preserve records and the ability to correct cases of error or sudden failure.

2 .Emergency handling, and developing detailed plans to meet any system failure. These plans detail the responsibilities of individuals and indicate alternative operating locations that can be used when needed.

3 .Identification cards, which are adhesive paper tags placed on the data storage medium to distinguish the file.

1- Application control procedures

This type of control procedures relates to the use of computers to carry out specific applications. These procedures can be manual or electronic procedures. These procedures are divided into three types:

A- **Input control procedures**: This ensures that the data received for processing by computer represents operations that have been properly authenticated and that the data is accurate, correct and complete at the time of entering it into the computer.

B- **Operation control procedures (processing)**: The purpose of these procedures is to confirm the credibility and accuracy of the electronic processing of data for the specific application. Specifically, these procedures aim to confirm that all operations have been processed under a specific authorization, that all operations that have been authenticated for automatic processing have been processed and nothing has been deleted from them, and that no unauthorized operations have been added to the operations that have been authorized for processing. Operation control procedures take many forms, including:

1. **Use of digital totals**: This is a control total that has no meaning for financial purposes, but it is a digital total used for control purposes.

2. **Test number**: It is used as a means of verifying the validity of the numbers that distinguish the record fields. For example: using a test number to verify the validity of customer account numbers in the bank.

C- **Output control procedures**: They aim to:

1. Ensure the reliability and validity of the outputs (information) that are produced after electronic data processing.

2. Confirm that these outputs have been delivered to employees authorized to use them only and not to persons not authorized to use them.

2- Database control procedures:

There are some control procedures specific to database systems, including:

A- The existence of control procedures that limit freedom of access to the database only by authorized persons.

B- Coordinating and controlling the activities of database users so that data control is proportionate to the importance of that data.

C- The participation of a large number of users in the same data files requires that there be strict control over those files to prevent change or loss.

d- Taking the necessary precautions to maintain the continuity of the system, such as:

1. Using the necessary protection programs, such as a firewall to prevent intrusion into the network by intruders, and anti-virus programs.

2. Having backup data and programs stored outside the work site.

3. Specific procedures taken in emergency situations, such as theft and loss of data or programs.

4. Providing treatment from outside the organization in the event of disasters.

Summary

ICT auditing requires a comprehensive approach that encompasses financial, performance and compliance aspects. While cost-effectiveness and compliance are key considerations, it is equally important to assess whether ICT is achieving the intended outcomes, providing value for money and meeting the needs of citizens and stakeholders. Given the interconnected nature of ICT infrastructure and the rapid growth of shared services

and inter-agency initiatives, auditors must work closely with relevant entities to ensure a unified and comprehensive approach to both internal and external oversight. By fostering collaboration and information sharing, auditors can enhance the impact of their audits and promote accountability across the ICT ecosystem.

The chapter reviewed the importance of auditing IT and electronic information systems, noting the importance of examining and assessing security, integrity and compliance with laws and regulations. The chapter also covered controls in this area and the importance of their strict application, with a focus on potential security risks and how to address and prevent them.

The chapter also focused on the IT audit process, risk assessment techniques and vulnerability analysis of information systems, including internal and external threats. The chapter also includes examples of common observations in IT audit reports, as well as the role of auditing in maintaining the confidentiality and reliability of information, ensuring its availability, and implementing security policies effectively. It also highlights the importance of documenting audit processes and providing recommendations to improve security and reduce potential risks, and highlights challenges and solutions in the field of IT and electronic information systems auditing.

Chapter Two
The Applied Study

Chapter Two
The Applied Study

2/1 Introduction

The aim of this research is to analyze the impact of information security audit policies on reducing the risks of electronic information systems in Egyptian banks, and to provide the necessary recommendations to enhance the security of information and data in these banks, by describing the initial data obtained by the researcher through preparing and distributing the questionnaire list that he relied on in collecting data, in addition to testing the research hypotheses and obtaining the results and providing recommendations that enhance information security in Egyptian banks.

2/2 Study hypotheses

Based on the aforementioned objectives, the study sought to test the validity of the following main hypothesis:

There is a role for information security audit policies in their dimensions (system validity, audit team duties, internal audit system reports, documentation and evidence, information security audit code of conduct, external audit) in reducing the risks of electronic information systems in Egyptian banks.

And the following sub-hypotheses:

1. There is a role for information security audit policies in their dimensions (system validity, audit team duties, internal audit system reports, documentation and evidence, information security audit code of conduct, external audit) in reducing the risks of entry in banks.

2. There is a role for information security audit policies in their dimensions (system validity, audit team duties, internal audit system reports, documentation and evidence, information security audit code of conduct, external audit) in reducing operational risks in banks.

3. There is a role for information security audit policies in their dimensions (system validity, audit team duties, internal audit system reports, documentation and evidence, information security audit code of conduct, external audit) in reducing output risks in banks.

4. There is a role for information security audit policies in their dimensions (system validity, audit team duties, internal audit system reports, documentation and evidence, information security audit code of conduct, external audit) in reducing environmental risks in banks.

2/3 Statistical methods used in the study

To achieve the objectives of the study, the researcher relied on some descriptive statistical methods, and some inferential statistical methods.

A. Descriptive statistical methods:

Some descriptive measures were relied upon to describe the research data as follows:

1. Arithmetic mean:

It is an indicator to determine the relative importance of each element of the question, and the relative weights that were assigned to the responses of the sample items to the survey questions using the following mathematical equation:

$$\bar{X} = \frac{\sum_{i=1}^{n} x}{n}$$

Where:

$\bar{x}$: The arithmetic mean of the relative weights.

$\sum_{i=1}^{n} x$: The sum of the relative weights determined by the responses.

n: The sample size.

1- Standard deviation:

It is one of the measures of dispersion, and is used as an indicator to determine the deviations of values from their arithmetic mean and is calculated by the square root of the average of the squares of the values from their arithmetic mean, and is useful in measuring dispersion or homogeneity between opinions, and homogeneity between opinions increases when the standard deviation decreases, and dispersion between opinions increases when the standard deviation increases, and is calculated as follows:

$$\sigma = \sqrt{\frac{\sum_{i=1}^{n}(x - \bar{x})^2}{n}}$$

Where refers to the standard deviation

A. Statistical inferential methods:

T-Test:

It is a test used to know the significant difference of the calculated arithmetic mean of the sample, in terms of whether it is significant or not. If

the significance level P-Value is less than 0.05, there is a significant difference or differences. However, if the significance value is greater than 0.05, there is no significant difference or differences.

SPSS version 25 gives the significance value P-Value, where it is compared to the significance value of 5%. If the significance value is smaller than the significance value of 5%, the hypothesis that there is a relationship between the two variables is accepted, and vice versa.

2/4 Survey List

In light of the data needed to test the study hypotheses, the researcher designed a questionnaire list, which included a set of phrases that measure the role of information security audit policies in its dimensions (system validity, audit team duties, internal audit system reports, documentation and evidence, information security audit code of conduct, external audit) in reducing the risks of electronic information systems in Egyptian banks, based on a set of phrases based on the five-point Likert scale.

2/5 Research community and sample

The study community consisted of members of the Supreme Audit Institution in Egypt and employees of the financial sector, the information technology sector, and the internal audit sector in an Egyptian bank. The study tool was distributed to a sample suitable and representative of the study community, and a random sample was taken from the study community where the inspection unit was represented by (managers, external auditors, accountants, department heads, internal auditors and their assistants, information technology employees) to whom (50) questionnaires were distributed, which were returned in full by 100%.

Each list received from the respondents was reviewed to ensure its completeness and suitability for inclusion in the statistical analysis. The following table illustrates this:

Table No (1)

Statement of the survey lists distributed, received and valid for statistical analysis

statement	Distributed Lists	Unreceived Lists	Received Lists	Excluded Lists	**Valid Lists**
count	**50**	**0**	**50**	**0**	**50**
%	**100**	**0**	**100**	**0**	**100**

It is clear from the previous table that the response rate reached (100%), and the lists valid for statistical analysis were (100%) of the total distributed lists, which amounted to (50) questionnaires.

2/6 Frequency and percentage tables

The researcher used these tables to deduce the number and percentages of responses from the respondents and put them in a table of two columns, the first representing the frequencies and the second the percentage of the sample size, as shown in the following tables:

Table No. (2) shows the number and percentage of respondents in the sample

Demographic variables		**Frequences**	**Percentage %**
Qualification	Bachelor	42	84
	Professional membership	2	4
	Master	4	8
	Doctorat	2	4

	Total	**50**	**100**
Gender	Male	30	60
	Female	20	40
	Total	**50**	**100**
Experience	5 years and under 10	2	4
	10 years and under 20	3	6
	20 years and above	45	90
	Total	**50**	**100**
Position	Financial manager	5	10
	Audit manager	10	20
	Internal, External auditor, Accountanta	20	40
	IT officers	15	30
	Total	**50**	**100**

2/7 Descriptive statistics

Description of the dimensions of the independent variable Information Security Audit Policies

This section aims to extract arithmetic means and standard deviations and indicate the degree of importance and arrangement of paragraphs to describe the trends of the study sample towards the dimensions of information security audit policies.

First dimension: System validity

Table (3): Arithmetic mean and standard deviation of the study sample individuals' response remotely

System validity

n	Statements	mean	Standard deviation	Approval degree	%	Rank
1	The public sector banks under consideration provide protection for the security and integrity of all components of the system.	3.61	0.914	medium	72.2	5
2	The public sector banks under study are keen to periodically subject system users to guidance lectures.	3.49	0.980	medium	69.8	6
3	The public sector banks under study separate the duties of systems analysts, systems operators and computer department staff.	3.63	0.981	medium	72.6	3
4	Public sector banks shall provide adequate and appropriate authority to the information security audit staff.	4.28	0.775	high	85.6	1
5	Public sector banks perform periodic maintenance of the physical components of the information system.	3.61	0.974	medium	72.2	4
6	Managers in public sector banks are keen to provide the internal auditor with the authority to conduct the audit process.	3.7	0.867	high	74	2
	Total	**3.72**	**0.573**	**high**	**74.4**	

The previous table indicates that this dimension achieved an arithmetic mean of (3.72) and a percentage of (74.4%) of the total scale area, with a standard deviation of (0.573), which indicates that the level of system validity came within the high level from the point of view of the study sample members, and the reason is that public sector banks grant appropriate and sufficient authority to the information security audit team, and managers in these banks are keen to provide the internal auditor with the authority to conduct the audit process.

Second dimension: Duties of the audit team

Table (4): Arithmetic mean and standard deviation Response of study sample members Remotely Duties of the audit team

n	Statements	mean	Standard deviation	Approval degree	%	Rank
7	Internal auditors in public sector banks have the necessary academic qualifications to perform their duties efficiently.	3.98	0.698	high	79.6	3
8	Public sector banks define the tasks and duties of the audit team and specify the powers assigned to them.	4.01	0.691	high	80.2	1
9	Public sector banks trust people who are responsible for checking and ensuring the security and integrity of information.	3.97	0.765	high	79.4	4
10	Departmental staff in public sector banks cooperate with internal auditors in dealing with information security tools.	3.84	0.915	high	76.8	6
11	Bank managements direct internal auditors to use modern technological tools	3.99	0.886	high	79.8	2
12	Auditors are keen to attend seminars and conferences on the information security and safety environment and obtain professional certificates in the field of information technology and auditing.	3.85	0.999	high	77	5
	Total	**3.94**	**0.607**	**high**	**78.8**	

Table (4) indicates that this dimension achieved an arithmetic mean of (3.94) and a percentage of (78.8%) of the total scale area, with a standard deviation of (0.607), which indicates that the level of the audit team's duties came within the high level from the point of view of the study sample members, and the reason is that public sector banks determine all the tasks, duties and powers of the audit team, and employees of the various departments cooperate with internal auditors to find a way to deal with information security tools.

The third dimension: Internal audit system reports

Table (5): The arithmetic mean and standard deviation of the study sample members' answers towards the dimension of internal audit system reports

n	Statements	mean	Standard deviation	Approval degree	%	Rank
13	Bank managements direct auditors to issue the internal auditor report as one of the information security policies.	4.6	0.628	high	92	1
14	The information security audit team is keen to issue a report with the audit results to address any deviations or errors.	4.14	0.687	high	82.8	2
15	Internal audit reports are submitted to the department manager in order to follow up on mandatory procedures to address any exceptions.	3.97	0.730	high	79.4	4
16	The Information Security Audit Team is keen to provide internal audit reports when needed.	3.85	0.921	high	77	5
17	The Internal Audit Department reports to the Board of Directors on the risk's banks are exposed to and how to avoid them.	4.1	0.788	high	73.6	3
18	The Information Security Audit Team is keen to review and audit all financial transactions at public sector banks.	3.68	0.887	high	73.6	6
	Total	**4.06**	**0.539**	**high**	**81.2**	

The previous table indicates that this dimension achieved an arithmetic mean of (4.06) and a percentage of (81.2) of the total scale area, with a standard deviation of (0.539), which indicates that the level of internal audit system reports came within the high level from the point of view of the study sample members, and the reason is that the administrations of public sector banks direct auditors to issue a report representing the results of the audit process to

address any deviations or errors, and the information security audit team in those banks is keen to audit and review all their financial transactions.

Fourth dimension: Documentation and evidence

Table (6): Arithmetic mean and standard deviation of the answers of the study sample members towards the documentation and evidence dimension

n	Statements	mean	Standard deviation	Approval degree	%	Rank
19	Public sector banks are keen to put in place instructions for documenting the audit process.	3.99	0.756	high	79.8	1
20	Public sector banks are keen to establish controls over documents and the sequence of data entry procedures into the system.	3.78	0.912	high	75.6	5
21	Public sector banks collect evidence from its primary source and verify the accuracy of the information contained therein.	3.93	0.824	high	78.6	3
22	Banks keep a copy of the processing programs in a convenient location and record the system output as a means of control.	3.64	0.863	medium	72.8	6
23	Public sector banks emphasize the need to document all procedures and mechanisms followed during the work on auditing information security.	3.95	0.901	high	79	2
24	Banks are keen to ensure that the evidence is appropriate and sufficient to obtain an information security report.	3.91	0.905	high	78.2	4
	Total	**3.78**	**0.649**	**high**	**77.4**	

The previous table indicates that this dimension achieved an arithmetic mean of (3.87) and a percentage of (77.4%) of the total scale area, with a standard deviation of (0.649), which indicates that the level of documentation and

evidence came within the high level from the point of view of the study sample members, and the reason is that these banks are working on developing instructions related to documenting their auditing process, keeping a copy of the processing programs in appropriate places, and recording the system outputs.

Fifth dimension: Code of Conduct for Information Security Audit

Table (7): Arithmetic mean and standard deviation of the study sample members' answers towards the dimension of the Code of Conduct for Information Security Audit

n	Statements	mean	Standard deviation	Approval degree	%	Rank
25	Public sector banks are committed to the Code of Conduct for Information Security Auditing.	3.74	0.844	high	74.8	5
26	Internal auditors in banks are keen to perform the duties assigned to them in a purposeful manner and with great care.	3.75	0.734	high	75	4
27	Internal auditors in banks are bound to maintain the confidentiality and privacy of the information collected.	3.68	1.027	high	73.6	6
28	Internal auditors in banks are keen to provide accurate results of the entire audit process.	3.82	0.894	high	76.4	2
29	Public sector banks support awareness efforts aimed at helping their customers develop their understanding of information systems security and management.	3.80	0.750	high	76	3
30	Public sector banks are subject to severe and deterrent penalties in case the auditor fails to work within the Code of Conduct for Information Security Audit.	4.06	0.937	high	81.2	1
	Total	**3.81**	**0.670**	**high**	**76.2**	

The previous table indicates that this dimension achieved an arithmetic mean of (3.81) and a percentage of (76.2%) of the total scale area, with a standard deviation of (0.670), which indicates that the level of the code of conduct for

information security auditing came within the high level from the point of view of the study sample members, and the reason is that banks are working on developing instructions related to documenting their auditing process, keeping a copy of the processing programs in appropriate places, and recording the system outputs.

Sixth dimension: External audit

Table (8): Arithmetic mean and standard deviation of the study sample members' answers towards the dimension of external audit of information technology

n	Statements	mean	Standard deviation	Approval degree	%	Rank
31	The external audit of the bank's information technology is carried out on an appropriate basis from 2 to 5 years.	3.74	0.844	high	74.8	5
32	External IT auditors perform their duties with purpose and utmost care.	3.75	0.734	high	75	4
33	External IT auditors follow IT standards, manuals and guidelines issued by international and local professional organizations.	3.68	1.027	high	73.6	6
34	External IT auditors ensure that they provide accurate results for the entire audit process.	3.82	0.894	high	76.4	2
35	The External IT Auditor's Report provides recommendations to help reduce the risks to banks' information systems.	3.80	0.750	high	76	3
36	External IT audit helps enhance information security and cybersecurity and reduces input risks, operational risks, output risks and environmental risks.	4.06	0.937	high	81.2	1
	Total	**3.81**	**0.670**	**high**	**76.2**	

The previous table indicates that this dimension achieved an arithmetic mean of (3.81) and a percentage of (76.2%) of the total scale area, with a standard deviation of (0.670), which indicates that the level of external auditing of information technology came within the high level from the point of view of the

study sample members, and the reason is that external auditing of information technology helps in enhancing information security and cyber security and reduces input risks, operational risks, output risks and environmental risks, and external information technology auditors are keen to provide accurate results for the audit process.

Second: Risks of electronic information systems

First field: Input risks

Table (9): Arithmetic mean and standard deviation of the response of the study sample members about input risks

n	Statements	mean	Standard deviation	Approval degree	%	Rank
37	Public sector banks are keen to hold training courses to educate data entry personnel on the methods and importance of maintaining information security.	3.68	0.768	high	73.6	6
38	Employees should not share the same password and each bank employee should be forced to change it periodically.	3.97	0.858	high	79.4	4
39	Information systems in banks review inputs, ensure their accuracy, and reduce the entry of incorrect data.	4.25	0.720	high	85	1
40	Banks are keen to control the process of entering and modifying data except by authorized employees.	4.11	0.787	high	82.2	2
41	Banks always benefit from technological developments in the areas of information systems protection programs such as encryption programs.	3.73	0.785	high	74.6	5
42	Banks use alarm devices to alert in case of unauthorized entry of data.	4.04	0.886	high	80.8	3
	Total	**3.96**	**0.635**	**high**	**79.2**	

The previous table indicates that this dimension achieved an arithmetic mean of (3.96) and a percentage of (79.2%) of the total scale area, with a standard deviation of (0.635), which indicates that the level of reducing data entry risks came within the high level from the point of view of the sample members.

Second field: Operational risks

Table (10) The arithmetic mean and standard deviation of the study sample members' responses to operational risks

n	Statements	mean	Standard deviation	Approval degree	%	Rank
43	Public sector banks have information systems that prevent data from being modified by unauthorized individuals.	4.00	0.848	high	80	5
44	Providing adequate protection in banks by using anti-virus software and firewalls.	4.33	0.694	high	86.6	3
45	Contact your Internet service provider to restore service as quickly as possible if it is cut off by banks.	4.73	0.450	high	94.6	1
46	Periodically check new software and CDs before inserting them into computers.	4.06	0.689	high	81.2	4
47	Banks have information systems that are able to predict and mitigate operational risks.	3.57	0.816	medium	71.4	6
48	Banks are keen to process data electronically without human intervention.	4.54	0.688	high	90.8	2
	Total	**4.21**	**0.476**	**high**	**84.2**	

The previous table indicates that this dimension achieved an arithmetic mean of (4.21) and a percentage of (84.2%) of the total scale area, with a standard deviation of (0.476), which indicates that the level of reducing operational risks came within the high level from the point of view of the sample members.

Third field: Output risks

Table (11): Arithmetic mean and standard deviation of the study sample members' responses towards output risks

n	Statements	mean	Standard deviation	Approval degree	%	Rank
49	Track the outputs of each process and attach supporting documents to prove its existence in the banks under investigation.	3.89	0.760	high	77.8	2
50	The accounting information systems of the banks under investigation prevent the modification or falsification of reports issued by the system.	3.05	0.922	medium	61	6
51	Government institutions have accounting information systems that are able to prevent the possibility of creating unrealistic outputs by employees.	3.78	0.764	high	75.6	4
52	Keep paper system outputs in secure, locked locations and archive them to prevent loss, theft or damage.	3.59	0.893	medium	71.8	5
53	Establishing rules and regulations that determine the distribution paths of reports resulting from the system in the banks under study.	3.80	0.820	high	76	3
54	Issuing confidential copies of the outputs of the information systems in the banks under investigation to facilitate inspection and evaluation processes and confront cases of theft or forgery.	3.9	0.781	high	78	1
	Total	**3.67**	**0.597**	**high**	**73.4**	

The previous table indicates that this dimension achieved an arithmetic mean of (367) and a percentage of (73.4%) of the total scale area, with a standard deviation of (0.597), which indicates that the level of reducing output risks came within the high level from the point of view of the sample members.

Fourth Domain: Environmental Risks

Table (12): Arithmetic mean and standard deviation of the study sample members' responses to environmental risks

n	Statements	mean	Standard deviation	Approval degree	%	Rank
55	There is sufficient awareness of how to deal with emergencies when natural disasters occur in the banks under study.	4.8	0.420	high	77.8	2
56	Banks develop a clear plan to anticipate damages caused by environmental risks and how to address and prevent them.	4.16	0.598	high	61	6
57	Government institutions management updates protection methods according to changes in the technology environment.	4.08	0.670	high	75.6	4
58	The internal auditor can issue directives to the management that the bank management must bear part of the external environmental risks resulting from mismanagement.	4.57	0.610	high	71.8	5
59	The banks under study are keen to develop plans to confront environmental factors such as earthquakes, hurricanes, floods and fires that affect the security and safety of electronic information systems.	4.10	0.607	high	76	3
60	The banks under study hold training courses on the security and safety of electronic information systems in the event of natural or unnatural disasters that may affect the operation of the system.	3.87	0.806	high	78	1
	Total	**4.26**	**0.393**	**high**	**85.2**	

The previous table indicates that this dimension achieved an arithmetic mean of (4.26) and a percentage of (85.2%) of the total scale area, with a standard deviation of (0.393), which indicates that the level of environmental risk reduction was within the high level from the point of view of the sample

members.

2/8 Inferential statistics

1- Testing the impact of information security audit policies with their dimensions in reducing the risks of electronic accounting information systems

Table (13): Results of testing the impact of information security audit policies with their dimensions in reducing the risks of electronic accounting information systems

Coefficient						ANOVA			Model Summery		
T Sig	T	Beta	Standard deviation	B	statemet	Df	F Sig	F	R2	R	Dependent variable
*0.00	5.501	0.239	0.033	0.179	System Validity	280/5	*0.00	110.291	0.663	0.814	Reducing the risks of electronic accounting information systems
0.911	0.122	0.006	0.041	0.005	Audit Team Duties						
*0.00	5.318	0.322	0.048	0.257	Audit Reports						
*0.00	3.625	0.196	0.036	0.130	Documentation and Evidence						
*0.00	3.688	0.206	0.036	0.132	Code of Conduct						
*Significant at significance level α≥0.05											
T-table value = 1.96						Table F value = 2.21					

The previous table indicates that there is a statistically significant effect of information security audit policies in reducing the risks of electronic accounting information systems through the F value of (110.291), which is greater than its tabular value of (2.21) and significant at the significance level (0.05≥a). The correlation coefficient also reached (814), indicating the existence of a strong relationship between information security audit policies and reducing the risks of electronic accounting information systems.

2- **Results of selecting the first sub-hypothesis**

Table (14): Results of testing the effect of information security audit policies

with their dimensions in reducing the risks of entry

Coefficient						ANOVA			Model Summery		
T Sig	T	Beta	Standard deviation	B	statement	Df	F Sig	F	R2	R	Dependent variable
*0.00	4.784	0.248	0.057	0.272	System Validity	280/5	*0.00	60.691	0.520	0.721	Reducing the risk of entry
0.847	0.193	0.013	0.072	0.014	Audit Team Duties						
*0.001	3.331	0.241	0.085	0.284	Audit Reports						
0.442	0.770	0.050	0.063	0.049	Documentation and Evidence						
*0.00	5.835	0.390	0.063	0.369	Code of Conduct						
*0.00	5.835	0.390	0.063	0.369	External audit						
*Significant at significance level α≥0.05											
T-table value = 1.96						Table F value = 2.21					

Table (14) represents the results of the statistical test of the model of this hypothesis, which is represented by the presence of a set of independent variables, namely the validity of the system, the duties of the audit team, the reports of the internal audit system, documentation and evidence, the code of conduct for information security auditing, external auditing, and one dependent variable representing the reduction of entry risks. The table indicates the presence of a statistically significant effect of information security audit policies in reducing entry risks through the F value of (60.691), which is greater than its table value of (221) and significant at a significance level of (0.05). The correlation coefficient also reached (72.1%), which indicates the presence of a strong relationship between information security audit policies and the reduction of entry risks.

3- Results of selecting the second sub-hypothesis:

Table (15): Results of testing the effect of information security audit policies

with their dimensions in reducing operational risks

Coefficient								ANOVA	Model Summery		
T Sig	T	Beta	Standard deviation	B	statement	Df	F Sig	F	R2	R	Depended variable
*0.00	3.894	0.216	0.046	0.179	System Validity	280/5	*0.00	45.945	0.451	0.671	Reducing the risk of operating
0.532	0.625	0.046	0.058	0.036	Audit Team Duties						
*0.004	2.941	0.228	0.068	0.201	Audit Reports						
*0.00	4.605	0.318	0.051	0.233	Documentation and Evidence						
0.815	0.234	0.017	0.051	0.012	Code of Conduct						
0.815	0.234	0.017	0.051	0.012	External audit						
*Significant at significance level α≥0.05											
T-table value = 1.96						Table F value = 2.21					

Table (15) represents the results of the statistical test of the model of this hypothesis, which is represented by the presence of a set of variables (system validity, audit team duties, internal audit system reports, documentation and evidence, code of conduct for information security auditing, external auditing, and one dependent variable representing reducing operational risks. The table indicates the presence of a statistically significant effect of information security audit policies in reducing operational risks through the F value of (45.945), which is greater than its table value of (2.21) and significant at a significance level of (0.05≥a). The correlation coefficient also reached (67.1%), which indicates the presence of a strong relationship between information security audit policies and reducing operational risks.

5- Results of selecting the third sub-hypothesis:

Table (16): Results of testing the effect of information security audit policies with their dimensions in reducing output risks

Coefficient						ANOVA			Model Summery		Dependent variable
T Sig	T	Beta	Standard deviation	B		Df	F Sig	F	R2	R	
*0.00	3.863	0.214	0.058	0.222	System Validity	28/50	*0.00	46.706	0.455	0.674	Reducing the risk of output
0.867	0.168	0.012	0.072	0.012	Audit Team Duties						
*0.001	3.490	0.269	0.085	0.298	Audit Reports						
0.096	1.672	0.115	0.063	0.106	Documentation and Evidence						
*0.007	2.731	0.194	0.063	0.173	Code of Conduct						
*0.007	2.731	0.194	0.063	0.173	External audit						
Significant at significance level α≥0.05*											
T-table value = 1.96						Table F value = 2.21					

Table (16) represents the results of the statistical test of the model of this hypothesis, which is represented by the presence of a set of independent variables, namely the validity of the system, the duties of the audit team, the internal audit system reports, documentation and evidence, the code of conduct for information security auditing, external auditing, and one dependent variable representing the reduction of output risks. The table indicates the presence of a statistically significant effect of information security audit policies in reducing output risks through a value of (46.706), which is greater than its tabular value of (2.21) and significant at a significance level of (0.05≥a). The correlation coefficient also reached (64.5%), which indicates the presence of a strong relationship between information security audit policies and the reduction of environmental risks.

6- Results of selecting the fourth sub-hypothesis

Table (17): Results of testing the impact of information security audit policies with their

dimensions in reducing environmental risks

Coefficient						ANOVA			Model Summery		
T Sig	T	Beta	الخطأ المعياري	B	statement	Df	F Sig	F	R2	R	المتغير التابع
0.304	1.030	0.059	0.039	0.040	System Validity	28/50	*0.00	39.830	0.416	0.645	Reducing the risk of environment
0.375	0.889	0.067	0.049	0.044	Audit Team Duties						
*0.00	4.210	0.336	0.058	0.245	Audit Reports						
*0.00	5.307	0.378	0.043	0.229	Documentation and Evidence						
0.981	0.024	0.002	0.043	0.001	Code of Conduct						
0.981	0.024	0.002	0.043	0.001	External audit						
Significant at significance level α≥0.05* •											
T-table value = 1.96						Table F value = 2.21					

Table (17) represents the results of the statistical test of this hypothesis model, which is represented by the presence of a set of independent variables, namely the validity of the system, the duties of the audit team, the internal audit system reports, documentation and evidence, the code of conduct for information security auditing, external auditing, and one dependent variable representing the reduction of environmental risks. The table indicates the existence of a statistically significant effect of information security auditing policies in reducing environmental risks through the F value of (39.83), which is greater than its tabular value of (2.21) and significant at a significance level of (0.05). The correlation coefficient also reached (64.5%), which indicates the existence of a strong relationship between information security auditing policies and the reduction of environmental risks. From the results of the statistical analysis of the main hypothesis and sub-hypotheses, it is clear that there is a role for information security auditing policies with their dimensions (system

validity, duties of the audit team, internal audit system reports, documentation and evidence, code of conduct for information security auditing, external auditing) in reducing the risks of electronic information systems in Egyptian banks, and a strong relationship between the study variables.

Chapter Three
Results & Recommendations

Chapter Three
Results and Recommendations

In this section, the researcher discussed the results and recommendations he reached, and therefore this section was divided into the following:

3/1: Results

3/2: Recommendations

3/1 Results

In light of the results of the analysis of the applied study data conducted by the researcher, the results can be presented as follows:

1- There is a statistically significant relationship between information security audit policies in their dimensions (system validity, audit team duties, internal audit system reports, documentation and evidence, information security audit code of conduct, external audit) and reducing the risks of electronic information systems in Egyptian banks.

2- Studies have shown that implementing regular IT system audits can significantly reduce cybersecurity risks and data breaches. Practical examples indicate that techniques such as periodic vulnerability scanning, threat assessment, and implementing necessary corrective actions can contribute to enhancing the security of electronic systems.

3- The importance of having a strong and independent regulatory framework for monitoring information systems, as supreme audit bodies can play a major role in defining security standards and practices, monitoring their implementation, and guiding companies and institutions to improve the security and reliability of their systems. Cooperation between the public and private sectors can also contribute to enhancing the effectiveness of monitoring efforts and improving information security. 4- Companies and organizations must deal with various challenges related to IT auditing, such as the development of cyber threats and new legislation related to data protection. An important opportunity is to take advantage of modern technological developments to enhance the ability of stakeholders to detect and respond to security threats.

4- Companies and organizations must implement multiple strategies to improve IT auditing operations, including hiring qualified personnel, adopting big data analysis techniques, and cooperating with specialized security service providers.

5- Evaluating the effectiveness of IT audits can help identify strengths and weaknesses and identify areas that need improvement. It is also important to exchange experiences and knowledge between companies and organizations to enhance a common understanding of best practices in the field of IT auditing.

6- Implementing IT audits can contribute to enhancing compliance with legislation and legal regulations related to data protection and information security. This may reduce the legal risks and financial consequences of security breaches.

7- IT auditing can contribute to enhancing communication and awareness of cybersecurity risks within organizations, and encouraging employees to participate in data protection efforts and report any inquiries or potential violations.

8- Through IT auditing, organizations can improve their readiness to respond to security incidents such as data breaches or cyber attacks. These strategies include advance planning and periodic exercises to confront security incidents and provide an effective response.

9- IT auditing can contribute to building trust and credibility in digital systems, whether within organizations or between customers and business partners. This can enhance electronic interactions and increase confidence in the use of technology.

10-Implementing IT audits can improve the efficiency and effectiveness of business operations, by reducing unplanned interruptions and downtime due to security issues, and enhancing communication and secure information exchange between different departments in the organization.

Recommendations

In light of the researcher's findings from the descriptive analysis, and review of studies, references and research, the researcher presents a set of recommendations that can be summarized as follows:

1- Enhancing employee awareness and training: Organizations must enhance their employees' awareness of the importance of information security and secure technology practices, and provide them with continuous training on cyber threats and how to deal with them.

2- Implementing periodic audit procedures: Institutions should conduct periodic audits of their systems and technologies to ensure that they are in line with the latest security standards and comply with legislation and regulations.

3- Enhancing cooperation with the highest auditing bodies: Companies and institutions should enhance cooperation with the highest auditing bodies and benefit from the guidelines and directives they provide to improve information security.

4- Adopting best practices and modern technologies: Institutions should use best practices and adopt modern technologies in implementing auditing processes and securing electronic systems.

5- Developing security incident response strategies: Institutions should develop specific and effective strategies for responding to security incidents, and conduct periodic training to examine and improve their response.

6- Leveraging data analytics and artificial intelligence: Companies and organizations can use data analytics and artificial intelligence technologies to enhance their ability to detect security threats and analyze unusual behavior within electronic systems. 17- Periodic updating of security policies and internal procedures: Organizations should regularly evaluate and update their internal security policies and procedures to ensure that they remain consistent with developments in cyber threats and legal requirements.

References

References

First: References in Arabic

International Guides and Standards

1- INTOSAI, 2022, INTOSAI Development Initiative Guide on IT Auditing for Supreme Audit Institutions.

2- INTOSAI, 2019, INTOSAI Framework for Professional Guidance.

3- International Federation of Accountants, 2019, International Auditing Standards.

4- American Institute of Internal Auditors, 2017, International Standards for the Professional Practice of Internal Auditing.

Books:

1- Al-Dhaiba, Ziad Abdel Halim and others, 2014, Information Systems in Control and Auditing, Dar Al-Masirah, Amman, Jordan.

2- Al-Sarna, Raad Hassan, 2021, Quality and Environmental Management Systems, University of Sham, Syria.

3- Al-Zaza, Naji Shukri, 2016, Information and Communication Technology: Structure and Protection, Dar Al-Quds for Printing and Distribution, Gaza, Palestine.

4- Imports, Khalaf Abdullah, 2019, Internal Audit Guide According to International Standards Issued by IIA (Al-Warraq Publishing and Distribution, Amman, Jordan.

5- Anwar, Ahmed, 2017, Introduction to Information Technology and Information Retrieval Basics, Dar Al-Thaqafa Al-Ilmiyyah, Alexandria, Egypt.

6- Juma, Ahmed Helmy, 2019, Introduction to Reasonable Assurance According to International Standards on Auditing, Dar Safaa for Publishing and Distribution, Amman, Jordan, Third Edition.

7- Suleiman, Ahmed Fouad, 2017, Information Technology for Business, Arab Center for Scientific Studies and Research, Egypt.

8- Sadiq, Dalal, and Al-Fattal, Hamid Nasser, 2019, Information Security, Dar Al-Yazouri Scientific Publishing and Distribution, Amman, Jordan.

9- Ali, Abdel-Wahab Nasr, and Shehata, Shehata Al-Sayed, Accounting Information

Systems (Introduction to Transactions and Information Technology Cycles), Accounting Department, Faculty of Commerce - Alexandria University, 2015.

10- Karasneh, Ibrahim, 2017, Basic and Contemporary Frameworks in Banking Supervision and Risk Management, Economic Policy Institute, Arab Monetary Fund, Abu Dhabi, UAE, Second Edition.

11- Manish, Agrawal, et al., 2018, Information Security and IT Risk Management, Translated by: Jaafar bin Ahmed Al-Alwan, Research and Studies Center - Institute of Public Administration, Kingdom of Saudi Arabia.

12- Younis, Zain, and Mustafa, Awadi, 2015, Internal Audit and Information Technology According to International Auditing Standards, Sakhri Printing Press, El Oued, Algeria.

Scientific thesis

1- Abu Al-Haija, Ahmed Adnan, 2017, The impact of the reliability of accounting information systems in light of the application of information technology governance on the profitability of Jordanian banks listed on the Amman Stock Exchange, PhD thesis, World Islamic Sciences University, College of Graduate Studies, Amman, 2017.

2- Abu Rumman, Enas Fawzi, 2021, The role of auditing in reducing the risks of electronic accounting information systems in Jordanian commercial banks, Master's thesis, College of Graduate Studies, Al-Balqa University, Jordan.

3- Abu Amr, Iman Hussein Hassan, 2023, The impact of information technology auditing on the effectiveness of accounting information systems in Jordanian commercial banks, PhD thesis, College of Graduate Studies, World Islamic Sciences University, Amman, Jordan.

4- Al-Bari, Walaa Awad Jazi, 2023, The Impact of Information Technology Auditing in Reducing External Audit Risks in Banks Listed on the Amman Stock Exchange, Master's Thesis, Al al-Bayt University, Amman, Jordan

5- Al-Awamri, Abeer Issa, 2022, The Impact of Integrating Information Security Governance and Trust Assurance Services on Reducing the Risks of Electronic Accounting Information Systems, Master's Thesis, Faculty of Commerce, Benha University, Egypt.

6- Al-Ilmi, Hossam Ahmed Mohamed, 2015, The Role of Computerized Accounting

Information Systems in the Efficiency and Effectiveness of External Auditing, Master's Thesis, Faculty of Commerce, Islamic University, Gaza, Palestine.

7- Al-Saadawi, Mohamed Abdullah Farag, 2017, Activating the Impact of Information Systems Governance in Reducing Information Systems Risks: A Field Study, Master's Thesis, Faculty of Commerce - Ain Shams University, Egypt.

8- Al-Munizel, Muhammad Hassan Mufleh, 2021, The Impact of Computerized Accounting Information Systems on Enhancing the Effectiveness of Internal Control in Jordanian Commercial Banks, Master's Thesis, College of Graduate Studies, University of Jerash, Jordan.

9- Al-Wahib, Abdul-Wahhab Mubarak, 2022, The Impact of Applying the COBIT5 Framework in Reducing Threats to the Security of Computerized Accounting Information Systems in Banks Operating in Kuwait, Master's Thesis, College of Graduate Studies, World Islamic Sciences and Education University, Jordan.

10- Hassan, Yasser Al-Tamimi, 2017, The Role of the Internal Auditor in Evaluating the Security of Accounting Information Systems in Light of Information Technology Governance with Application to the Suez Canal Authority in Port Said, Master's Thesis, Faculty of Commerce, University of Port Said, Egypt.

11- Muhammad, Mirghani Al-Sheikh Omar, 2017, Methods of Reviewing Electronic Accounting Information Systems and Their Impact on the Quality of External Audit: A Field Study, Master's Thesis, College of Graduate Studies, University of Nilein, Sudan.

Articles:

1- Abu Shaiba, Ibrahim Ali, Al-Futtaimi, Muhammad Miftah, 2017, Risks of Using Electronic Accounting Information Systems: A Field Study on Commercial Banks in Misurata Municipality, Journal of Economics and Business Studies, Faculty of Economics and Political Science, Misurata University, Fifth Year, Special Issue.

2- Al-Jarbou, Abdullah Muhammad, 2023, Crimes of Deliberate Attack on the Integrity of Electronic Information Systems According to the Saudi System (An Analytical and Applied Study), Journal of Jurisprudential and Legal Research, Volume 35, Issue 43, Faculty of Sharia and Law, Al-Azhar University, Egypt.

3- Al-Azmi, Abdullah Faleh, 2022, The Role of Activating Information Technology Governance in Securing Accounting Information from Electronic Risks in the Age of

Digitization, Scientific Journal of Financial and Administrative Studies and Research, Volume Thirteen, Issue Two, Faculty of Commerce, Sadat City University, Egypt.

4- Al-Tayeb, Al-Sadiq Muhammad Al-Salem, and Al-Siddiq, Babiker Ibrahim, 2014, The Quality of External Auditing in the Light of the Electronic Operating Environment of Financial Data "A Theoretical Study, Journal of Economic Sciences, Issue 15(2), Sudan University of Science and Technology.

5- Al-Marri, Rashid Muhammad, 2023, The Impact of Information Technology on the Security System and Internal Control, Journal of Jurisprudential and Legal Research, Volume 35, Issue 40, Faculty of Sharia and Law, Al-Azhar University, Egypt.

6- Al-Mutairi, Fahd Khalid, 2023, The Impact of Integration between the Reliability of Electronic Accounting Information Systems and the Application of Governance Mechanisms on the Profitability of Kuwaiti Commercial Banks (A Field Study), Scientific Journal of Financial and Administrative Studies and Research, Volume 15, Issue 3, Faculty of Commerce, Sadat City University, Egypt.

7- Al-Naqbi, Jamal Muhammad, and Al-Masabi, Sultan Muhammad, 2023, Technical and Legal Aspects of Electronic Information Systems, Journal of the Higher Institute for Qualitative Studies, Volume 3, Issue 4, Egypt.

8- Balqasim, Muharib Saad Suleiman, Hussein, Ahmed Muhammad Salim, 2017, The Reality of Electronic Accounting Information Systems Security Risks in Libyan Commercial Banks in Al-Bayda City, The First International Scientific Conference: Hedging and Risk Management in the Islamic Financial Industry, Al-Sanabel Center for Research and Human Resources Development and Bayan Center for Islamic Financial Engineering, Amman, Jordan.

9- Habib, Samar, 2022, The Role of Accounting and Cloud Auditing Standards in Ensuring Data and Information Security: A Field Study from the Perspective of External Auditors in Syria, Tishreen University Journal of Economic and Legal Sciences, Volume 44, Issue 6, Tishreen University, Syria.

10- Hussein, Mahmoud Abdel Rahim, 2020, The Influential Role of Information Technology Governance as an Intervening Variable in the Relationship between Internal Auditing as a Value-Adding Activity and Reducing the Risks of Electronic Accounting Information Systems, Journal of Accounting Studies and Research, Faculty of Commerce, Benha University - Issue Two.

11- Daif Allah, Muhammad Al-Hadi, 2021, The Impact of Information Technology

Governance on Reducing Accounting Information System Risks, Journal of Financial, Accounting and Administrative Studies, Volume 8, Issue 1, University of Umm Al-Bouaghi, Algeria.

12- Ghanem, Sami Muhammad Ahmad, "Towards an Accounting Standard for Information Technology Governance in Light of the Development of Communications Technology and Information Exchange - A Field Study", Accounting Thought Journal, Accounting and Auditing Department, Faculty of Commerce, Ain Shams University, Issue Three - Part One, October 2017.

13- Qardash, Abbas, and Qanso, Hassan, 2023, The Impact of Computerized Accounting Information Systems on Investment Decision Making, Arab Journal of Humanities and Social Sciences, Issue 21, Al-Sunbula Center for Research and Studies, Amman - Jordan.

14- Karso, Arzaq Ayoub, 2023, Obstacles to Auditing Electronic Accounting Information Systems from the Perspective of Auditors Working in the Post and the Ministry of Finance in Light of the Corona Pandemic in Gaza, Afro-Asian Journal of Scientific Research, Volume One, Issue Four, African Academy for Advanced Studies, Turkey.

15- Heba Gamal Hashem Ali, 2023, A Proposed Procedural Approach to Measuring the Extent of the External Auditor's Response to Cyber Risks in an Establishment Client, Scientific Journal of Financial and Commercial Studies and Research, Volume 4, Issue 2, Faculty of Commerce, Suez Canal University, Egypt.

Second: References in English

Books:

1. Chris, Davis, and others, 2011, **IT Auditing: using controls to protect information assets**, Mc Graw Hill, 2011, second édition.
2. Davis, Robert E., 2021, **Auditing Information and Cyber Security Governance: A Controls-Based Approach**, CRC Press, Taylor & Francis Group, LLC, New York, USA.
3. Engel, Barak, 2024, **Why CISOs Fail (Internal Audit and IT Audit)**, CRC Press, Taylor & Francis Group, LLC, New York, USA.

4. Gantz, Stephen D., 2014, **The Basics of IT Audit. Purposes, Processes, and Practical Information**, Syngress
5. Hernan, Murdock, 2019, **Auditor essentials 100 concepts, tips, tools, and techniques for success**, CRC Press, Taylor & Francis Group, LLC, New York, USA.
6. ISACA, CISA Review Manual, 2019, 27 th edition, USA.

Periodecals:

1. Al-Fatlawi Q.Ali, Salman, Dawood, Almagtome, Akeel, 2021, Accounting Information Security and IT Governance Under COBIT5 Framework: A Case Study, **Faculty of Administration and Economics**, University of Kufa, Najaf, Iraq, Vol.18.
   Available at: https://www.researchgate.net, Retrieved at: 30-2-2024.
2. Alsaleem, Enas Amjed, & Husin, Norhayati Mat, 2023, The Impact of Information Technology Governance Under Cobit-5 Framework on Reducing the Audit Risk in Jordanian Companies, **International Journal of Professional Business Review**, Volume 8, Issue 2, Miami, USA.
3. Bradford, M., et al, 2020, Using generalized audit software to detect material misstatements, control deficiencies and fraud: How financial and IT auditors perceive net audit benefits, **Managerial Auditing Journal**, Vol. 35 No. 4. https://doi.org/10.1108/MAJ-05-2019-2277
4. Hossin, Adel M.& Ayedh, Abdellah M., 2016, The Risks of Electronic Accounting Information System in the Centeral Bank of Libya, **South East Asia Journal of Contemporary Business, Economic & Law**, Vol.1, No.1.
5. Hussain, M. Ali, 2013, A Study of Information Security in E-Commerce Application, **International Journal of Computer Engineering Science (IJCES),** Vol.3, Issue3.
6. Institute of Internal Auditors (IIA), 2016, International Standards for the Professional Practice of Internal Auditing Standards.

7. Krishna, D Jadhav, 2023, The Role of Cybersecurity Audits in Managing Company Systems and Applications,
8. Mirwali Azizi, Hakimi, M., Frishta Amiri, & Amir Kror Shahidzay, 2024, The Role of IT (Information Technology) Audit in Digital Transformation: Opportunities and Challenges. **Open Access Indonesia Journal of Social Sciences**, volume 7, issue 2.
9. Mohammad Aljanabi & et al, 2023, The Purpose of Cybersecurity Governance in the Digital Transformation of Public Services and Protecting the Digital Environment, **Mesopotamian journal of Cybersecurity**, vol.2023.
10. Pandzo, Alica, & Taljanovic, Kemal, 2013, IT Governance and IT Auditing Practice in Commercial Banks in Bosnia and Herzegovina, **Recent Advances in Information Science Jounal**.
11. Richard, Brisebois, 2015, What is IT Governence and why is it important for the IS auditor, **research journal of recent sciences**, vol. 09, issue 15, Information Systems Audit and Control Association (ISACA).
12. Rabii, Hamza, 2023, The Contribution of IT Audit to Data Governance, **Journal of Namibian Studies**, V. 36, issue S 2, Society of Cultural Studies and Social Sciences, Hong Kong
13. Slapnicar, Sergeja, & et al, 2022, Effectiveness of cybersecurity audit, **International Journal of Accounting Information Systems**, Volume 44, Issue 8, Elsevier Inc.
14. Taherdoost, Hamed, 2022, Understanding Cybersecurity Frameworks and Information Security Standards: A Review and Comprehensive Overview, Volume 11, Issue 14, **MDPI**, Basel, Switzerland.
15. Yohannes, Kurniawan & Archie Mulyawan, 2023, The Role of External Auditors in Improving Cybersecurity of the Companies through Internal Control in Financial Reporting, **Journal of System and Management Sciences**, Vol. 13, No. 1.

Training Course:

1- EUROSAI, ITWG, 2023, IT audit for non IT auditors, Training Course.