

Received: October 2023 Accepted: December 2023

DOI: <https://doi.org/10.58262/ks.v12i1.106>

Evaluation of the System of the Internal Control for the Electronic Accounting Information System according to the framework of the Committee of Sponsoring Organizations (COSO) Proposed Model

Amna Abbas Odeh¹, Prof. Dr. Khawla Hussein Hamdan²

Abstract

The research aims to identify internal control according to the framework of the Committee of Sponsoring Organizations (COSO) and the Electronic Accounting Information System and to evaluate the Internal Control over the Electronic Accounting Information System for economic units according to a proposed survey questionnaire that contains a set of questions for the elements of the framework (Control Environment, Risk Evaluation, Information and Communication, Control Activities, Monitoring Activities) and applied to the online program for salary clause (Key Card system). The research reached a number of conclusions. The most important conclusion is that the procedures of the Electronic Accounting Information System were not classified according to the elements of the framework of the Committee of Sponsoring Organizations (COSO). By applying the proposed model to the salaries of the department of education, the risks of the internal control, lack of effectiveness, were recorded at rates of (91%, 85%, 91%, 76%, 80%) for the elements (Control Environment, Risk Evaluation, Information and Communication, Control Activities, Monitoring Activities).

Keywords: Internal Control, Electronic Accounting Information System, framework of the Committee of Sponsoring Organizations (COSO).

Introduction

Economic units are units that have an economic impact on the service sector. Therefore, it has become important to pay attention to the Internal Control System that uses the Electronic Accounting Information System to increase its effectiveness and reduce risks. Therefore, the Committee of Sponsoring Organizations (COSO), which are professional organizations, sought to issue an Internal Control Framework in 1992, entitled Internal Control, an integrated framework that includes specific elements such as (Control Environment, Risk Evaluation, Information and Communication, Control Activities, Monitoring Activities) and principles for each element through which the strengths and weaknesses of internal control may be identified.

The research was organized into three main segments: First Segment: Research Methodology and Previous Studies, Second Segment: The theoretical internal control framework according to the framework of the Committee of Sponsoring Organizations (COSO) and the Electronic Accounting Information System, Third Segment: Evaluating Internal Control according to the

¹ Higher Institute of Accounting and Financial Studies - Baghdad
Email: Amna.Awda1701@pgiafs.uobaghdad.edu.iq

² Higher Institute of Accounting and Financial Studies - Baghdad
Email: Dr.kawla@pgiafs.uobaghdad.edu.iq

framework of the Committee of Sponsoring Organizations (COSO) for the Electronic Accounting Information System. A proposed model to be applied to the General Directorate of Education in Baghdad, Al-Karkh, Third, Salaries Clause.

First Segment: Research Methodology and Previous Studies

1-1: Research Methodology

1-1-1: Research Topic

Global professional organizations have paid attention to internal control. The Committee of Sponsoring Organizations (COSO) issued an internal control framework entitled Internal Control, which is an integrated framework for the purpose of improving the effectiveness of the performance of economic units, and can be applied to electronic operating systems in economic units in order to ensure that it adheres to the laws, regulations and instructions and that it achieves its desired objectives. Although the Financial Accounting Standards Board in Iraq's environment issued Audit No. (4) "Study and Evaluation of the Internal Control System in 2000 and updated it in 2020 according to the elements of the framework of the Committee of Sponsoring Organizations (COSO). However, the survey questionnaire did not include questions related to internal control under electronic operation. From the above-mentioned, the research topic is determined as follows:

The lack of a model for evaluating the internal control of electronic operating systems in economic units that takes into account the elements of internal control in accordance with the framework of the Committee of Sponsoring Organizations (COSO).

1-1-2: Research Objectives

A- Determining internal control according to the framework of the Committee of Sponsoring Organizations (COSO) and the electronic accounting information system in economic units.

B- Preparing the proposed questions for the internal control evaluation survey questionnaire for the electronic accounting information system for economic units and taking into account the internal control elements according to the framework of the Committee of Sponsoring Organizations (COSO) and applying it to the salaries clause for the research sample.

1-1-3 Significance of the Research

The importance of the research lies in preparing an internal control survey questionnaire of electronic operating systems in economic unit, which takes into account the elements of internal control according to the framework of the Committee of Sponsoring Organizations (COSO), which is used to evaluate it in order to determine the effectiveness of internal control of electronic operating systems to achieve the objectives of the economic units.

1-1-4: Hypothesis of Research

The research is based on the hypothesis, which is "preparing a proposed model in order to evaluate the internal control of electronic operating systems in economic units in accordance with the framework of the Committee of Sponsoring Organizations (COSO) and its application contributes to identifying the strengths and weaknesses of the internal control elements in order to address them in order to achieve the desired objectives of electronic operating systems."

1-2 Previous Studies

The study by (Fattah & Mohammed, 2012: 234,251) aimed to "Analyzing the reality of the internal control system in the surveyed company in order to determine the efficiency of the internal control system. The descriptive approach and interview were adopted in the analysis and measurement of the results. One of the most important conclusions reached by the study is the lack of specialized staff in maintenance the electrical and mechanical devices, and the presence of records for the manual system does not achieve the desired objective". The study by (Al-Taie & Muhammad, 2017: 129,155) aimed to "Discovering the current status of the internal control systems in Iraqi banks, evaluating the degree of effectiveness of procedures and controls for electronic accounting information systems, and determining the extent to which the characteristics of the control system for those information systems are compatible with the requirements and procedures for Iraqi banks, One of the most important conclusions reached by the study is that inadequate development and maintenance procedures for electronic accounting systems, as well as the occurrence of risks to electronic accounting information systems due to the lack of awareness, experience and employees training, the lack of clear, written control procedures for management, and the presence of weakness in applying control procedures regarding unauthorized access to the system, specifically, procedures for encrypting data, specifying and canceling the password, and trying to enter the computer room". The study by (Hussein & Muhammad, 2018: 1) aimed to "the possibility of activating the role of modern information systems through developing a model and mechanism through which the essential information about taxpayers is collected, and on the basis of which the taxpayers inventory process can carried out accurately and to clarify the importance of the outputs of computerized information systems. It relied on previous studies and the literature related to the research topic to collect data. The most important conclusions of the study are the employees' lack of academic and practical qualifications in high specialization in computerized information systems, and the failure to enter the available tax information and enter it into the computer in a high programmed manner for the purpose of storing and presenting it when needed, despite the availability of computers". The study by (Hamdan, 2020:4792) aimed to "Introducing Islamic finance and sustainable development. From the operational side, it aims to evaluate the performance of the Iraqi Islamic Bank for Investment & Development according to the dimensions of sustainable development (social, economic, environmental and institutional). The most important conclusions are that the Iraqi Bank for Investment & Development also contributed to the bank's participation with other banks in institutions and the purchase of advanced technology, including electronic payment and clearing". The study by (Al-Sharaida & Al-Samarrai, 2021: 5743) aimed to "Explain the relation between the use of automated accounting systems technology and its impact on enhancing the effectiveness of the internal control system in a sample of Bahraini universities in light of the rapid change in the e-business environment. The analytical approach was used to collect data in this research. The study found that 93% of the total sample fully agreed that the use of automated accounting contributes significantly to enhancing the effectiveness of the internal control system". The study by (Yousif, Mohammed,2022:4919)" The result of this research is that the internal audit is vital since knowing all the bank's data via its responsibility has an influential role in governance corporation, and it supports the senior management in the decision-making task as an acquisition decision". The study by (Hamdan, 2022:5743) aimed to "Learning about the elements of internal control of the Committee of Sponsoring Organizations which are (Control Environment, Risk Evaluation, Control Activities, Information and Communication,

and Monitoring Activities) and the Sendai Framework for Disaster Risk Reduction and define the degree of commitment to internal control of companies. Management of disasters in Iraqi environmental priorities within the Sendai Framework for Disaster Risk Reduction (SF-DRR)". The most important conclusions are the lack of a database for the numbers of victims and missing persons and the number of destroyed homes. There is no disaster risk reduction law and the Civil Defense Law is not activated. There is no national disaster preparation plan. There is no special budget for disaster risk management". The study by (Al-Jaboul, Abdel Majeed, 2023: 190-191) aimed to "Learning about the role of the external auditor in audit oversight in light of electronic accounting systems. They use the descriptive and analytical approach in collecting data. The study reached a strong agreement on the role of the external auditor in monitoring internal control, and agreement on the importance of electronic accounting systems". The study by (Helio, Abdullah, 2023: 184; Stedman et al., 2023)"The research aims to explain the role of cloud computing technology in facilitating the application of international financial reporting standards in Iraqi banks, by preparing a checklist that included a set of paragraphs to measure the level of application of IFRSs. In those banks and then the need to use cloud computing technology, and the researchers reached a set of conclusions, including, that cloud computing technology has a role in facilitating the application of international financial reporting standards in the banks, the research sample, because of the ease it provides in preparing and saving accounting information and the possibility of accessing it in any time and from any place where the Internet service is available".

Second Segment: The Theoretical Framework of Internal Control within the Framework of the Committee of Sponsoring Organizations (COSO) and the Electronic Accounting Information System for Economic Units

2-1 Internal Control within the Framework of the Committee of Sponsoring Organizations (COSO)

Before discussing the definition of internal control, we must know the meaning of (COSO), which is an abbreviation for (Committee of Sponsoring Organization of the Tread Way Commission), meaning it is the committee that consists of professional bodies in the accounting and financial field in the United States. The American Institutions Welfare Committee was named to provide a comprehensive vision of the concept of internal control and evaluation of internal control (Elias, 2017: 9), Internal control is considered a continuous process that affects all aspects of the institution and is considered one of the pillars of modern management and represents an important position as it culminates in administrative work, which in turn is not complete except by installing an effective control system that guarantees achieving a satisfactory level of performance (Nasima, 2019-2020: 3).

2-1-1 Definitions for the Internal Control

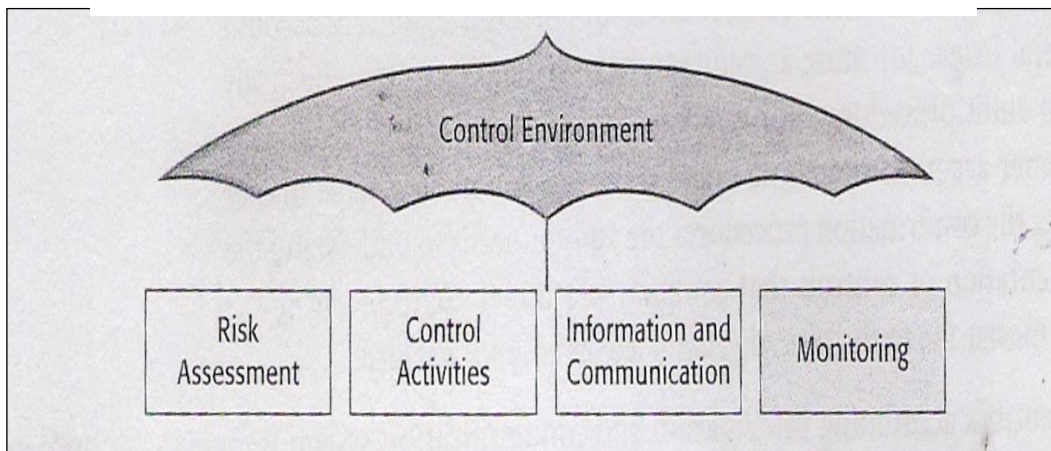
Many researchers and writers have provided a set of definitions for the Internal Control such as:

" These are processes that are influenced by the organization's board of directors, management, and other individuals in the organization and are designed to provide reasonable assurance that the organization is achieving its operational, financial, and compliance objectives (Al-Ramahi, 2023: 114-117), It has also been defined as "A process designed by the board of directors, management and other employees to provide reasonable assurance about the achievement of

objectives, namely the reliability of financial reporting, efficiency, effectiveness, and compliance with applicable laws and regulations” (Robertson&Louwers,2002: 144), It has also been defined as “A set of activities, procedures and policies that aim to verify the ability of the economic unit to achieve its set goals and disclose various financial and non-financial information with a high level of reliability through compliance with regulations, laws, regulations and policies” (Al-Basha, 2023: 159), Paragraph 4 of Standard 3402 (Assurance reports on control tools in a service Organization) defines internal control as" A mechanism designed, applied and maintained by those charged with governance, and other employees to provide reasonable assurance of achieving the Organization’s objectives with respect to approving financial report and the effectiveness of operations and compliance with applicable laws and regulations" (IFAC, 2023:219).

2-1-2: Internal Control Components

Internal control includes five basic components designed and implemented by management to provide appropriate assurance that the objectives of internal control are achieved. These components are (Al-Tamimi, 2018: 65) It can be displayed as in the figure below (Arens&etal.,2012: 316):



Source: Arens, Alvin&Elder, Randal&Beasley, Mark, 2012, "Auditing and Assurance Services", Pearson Education, Inc.

A - Control Environment

It is the basis for all other components of internal control (Yassin and Mansour, 2022: 233), The control environment is defined as" the general position of managers and management, their perceptions, and their actions related to the internal control system and its importance to the organization" (Rifa'a, 2017: 55) , Paragraphs (A108 & 66Z) of the International Standard for Assurance Engagements (ISAE) 3402 states that the auditor’s assessment of the control environment as it relates to the use of information technology includes several matters (IFAC, 2023: 365):

First: Whether the governance applied to information technology is proportional to the nature of the organization and its business operations supported by information technology, including the extent of the complexity of the platform or infrastructure of the organization’s technologies and the extent to which the organization reliance on information technology

applications to support the preparation of its financial report.

Second: The administrative organizational structure regarding information technology and the resources allocated to it. Given the different ways in which information technology is used and its assessment of acceptable levels of risk to the security of financial records and the completeness and reliability of the financial intelligence produced, the auditor must know a number of matters in order to understand the control environment, which are:

As for what was stated in Paragraph (8) of the International Auditing Practice Statement 1013 (IAPS, 2002: 221), it stated the following:

- (1) Involve those charged with governance and consider aligning the Information Technology strategy with the comprehensive strategy of the audited entity.
- (2) Whether the Information Technology application supports the activity of the audited entity and whether it is intended to make current activities more efficient and obtain future improvements.
- (3) Sources of funding for the audited entity and how and by what means it can be obtained.
- (4) Management's assessment of how information technology impacts the financial and organizational requirements of the audited entity.
- (5) Management's position on risks and how this affects the risk profile of the audited entity.
- (6) Management's commitment to establishing relevant best practice codes or developing specific programs.

B- Risk Evaluation

All components of internal control, starting from the control environment to Monitoring activities, must be subject to an assessment of the risks they contain (Al-Ghanoudi, 2020: 11),⁷International Standard on Auditing (ISA) 315 (Identifying and Evaluating Risks of Material Perversion) many of its paragraphs include information technology risks and how to evaluate those risks. Paragraphs (19 & 64A) include that control risks in information systems may occur as a result of the potential failure technology – based Information Technology controls that have been by the audited entity. For example, the audited entity may adopt an information system for the purpose of limiting access to confidential data of authorized individuals by providing the name of the person authorized to enter for the purpose of auditing and entering the specified password. The control risk in this case is that the user's name and specified password are not secure enough and could be guessed by unauthorized person through repeated attempts, leading to a lack of confidentiality and a potential negative impact on the entity.

Therefore, to achieve the goals, the entity must use a secure password that contains a set of alphabets, numbers, and special symbols. The most important risks caused by information technology to internal control in the organization are the following:

First: Relying on systems or programs that process data inaccurately, or process inaccurate data, or both of them.

Second: Unauthorized access to data, which may lead to the destruction of such data or the occurrence of improper changes in it, including recording unauthorized or non-existent transactions or recording transactions inaccurately. Some risks may arise when multiple users have accessed a shared database and the possibility of fraud by employees, in addition to the risk of making unauthorized changes to or failing to make the necessary changes to the data of main files, systems and programs.

Third: The possibility of IT employees obtaining access privileges that exceed those necessary to perform the tasks assigned to them, which leads to disruption of the segregation of duties.

Fourth: Inappropriate manual intervention.

Fifth: The possibility of losing data or the inability to access data, when needed, due to the spread of information technology risks, including virus attacks and others.

Sixth: Loss of integrity of transaction due to the lack of an appropriate audit record, whether paper or electronic.

Seventh: Incorrect accounting policies, such as misunderstanding of complex contractual arrangements or lack of knowledge in dealing with allocated allocations and revenue recognition issues.

Eighth: Non-compliance with taxes and other legal and regulatory requirements.

Ninth: Exposure to natural or non-natural faults in the information technology infrastructure. (IFAC,2023: 216-236))

Hamdan considers that "Risk Evaluation is vital for internal control because it enables senior management to identify and alleviate potential risks" (Hamdan, 2022: 5743), While (Al-Ahmedi & AL-Mamouri), see the necessity of establishing an electronic risk management department by developing an effective framework to identify, evaluate, analyze and document electronic risks in order to manage, dominate and control it or take administrative actions to alleviate it. (Al-Ahmedi, AL-Mamouri, 20:2023)

C- Control Activities

The trends, standards, strategies and options established by management are considered control activities (Mohamed and Abdel Karim, 2020: 534), Statement No. 1013 of the International Auditing Practice Statement (IAPS) includes several paragraphs on how to deal with information technology risks, including paragraph (20): The Information Technology Department establishes several procedures to face risks that arise when using information technology by establishing or preparing an appropriate infrastructure and establishing appropriate relevant controls, in general. These procedures include the following:

First: Verifying the identity of final users and system operators.

Second: Ensuring the accuracy and completeness of the transactions.

Third: Obtaining and reviewing the contractual stipulations and reviewing the requirements and instructions for implementing the budget to know how to deal with allocations and revenues.

Fourth: Dealing with accredited organizations and bodies and developing protocols related to the security and protection of information. The Paragraph (28) included providing the necessary security protection to ensure the protection and safety of information by providing an information technology infrastructure such as organizational controls related to information security policy, information security risk evaluation, standards, measures, actions and procedures through which systems are maintained, such as the use of digital IDs and passwords that are difficult for those who have the capacity and efficacy in field of information technology to know, and the auditor must provide this type of protection by taking several matters into account.

First: Effective use of anti-virus protection programs to protect its systems from entering unauthorized or harmful data electronically.

Second: Effective use of encryption.

Third: Maintaining the privacy and security of transmissions by licensing decryption keys.

Fourth: Prevent misuse of encryption technology by controlling and protecting private decryption keys.

Fifth: Controls for developing and executing systems used to support information technology activities.

Sixth: The effectiveness of the security controls in terms of their ability to counter cyberattacks.

Seventh: Paragraph (31) included the suitability of the control environment for procedures such as the use of technically advanced encryption systems, which would not be effective if a set of control activities were implemented, including:

- (1) Input Validation.
- (2) Preventing duplication in recording transactions or omission of transactions.
- (3) Ensure that transactions are completed before entering into the processing process in terms of approvals and ensure the availability of funds to conduct transactions.
- (4) Prevent incomplete processing, such as recording the document number and date, transactor, the amount allocated, the instrument number, and conformity both sides of the transaction.
- (5) Ensure proper distribution of transaction details across multiple systems in a consolidated network, e.g. data is distributed centrally and information is sent to various relevant departments.
- (6) Make sure that records are kept, backed up and secured properly.

The statement included, in many of its paragraphs, that there are several benefits when providing controls to the entity that uses information technology, such as:

A: Reducing risks: Paragraph (25) ensures that the use of internal control helps reduce many of the risks associated with information technology activities, as the auditor sometimes takes into account the control environment and control procedures that the entity has applied to information technology activities to reach assurances about the financial statements, such as:

If the size of transactions is large enough.

Not maintaining electronic evidence that includes the audit process.

The auditor has concluded that it is unable to reduce audit risks to a low or acceptable level using substantive procedures.

B- Providing information security: Paragraph (32) included that the presence of internal control helps provide security and safety for transactions and coordinate operations. The latter means integrating different information technology systems with each other and then effectively working as one system in the rapidly changing information technology environment, in addition to ensuring access to records relevant to the entity's needs and audit purposes.

C- Providing protection for information: Paragraph (27) included that the presence of internal control that provide a security and safety factor is important in the event that there are third parties able to use advanced methods through which they can access the information of the audited entity that has been secured to the extent that authorization, credibility, confidentiality,

integrity and availability requirements are met.

4- Achieving the integrity of transactions: Paragraph (29) included that the design of organizational controls in the information technology environment helps to achieve the integrity of transactions because the auditor takes into account the completeness, accuracy, and authorization of the information submitted for registration and processing in the financial records of the audited entity, because it affects the level of complexity of information technology activities and the nature and the extent of risks related to recording transactions electronically (IAPS, 2002: 226-228), "Techniques that help you figure out how much something costs are easier to get if you know how to use them"(Bediwi & et al, 2022: 6339)

D- Information and Communications

Information is necessary for any organization to carry out its internal control responsibilities in order to achieve its goals (Al-Ramahi, Nazal Mahmoud, 2016:475), As for communication, control over information technology requires selecting qualified employees for technical work, defining job description for them, informing them of the importance of the tasks assigned to them, and holding training courses for them to achieve the communication process (Piazza, 2014: 49). As well as Communication is a recurring process of obtaining, presenting and exchanging the necessary information (Al-Ramahi, Nazal Mahmoud, 2016:475), information must be recorded and communicated to management and others who need it within the economic unit in a form and time frame that helps them carry out internal control and other responsibilities (Thabet, Thabet Hassan, Chanshul, 2022:246).

E- Monitoring Activities

Monitoring activities aim to find out whether the control activities related to the five elements are going well (Fateeh, 2016: 11), By evaluating the quality of monitoring of the internal control system from two aspects: The first: continuous evaluations through regular management and supervision activities and the actions of other individuals charged with this area , The second: separate evaluations, the scope and frequency of which are determined based on the assessment of risk and the effectiveness of continuous monitoring procedures (Al-Jabali, 2022: 154), Paragraph (63A) of the International Standard on Auditing (ISA) 315 stated that, by reviewing the internal control tools or components (Control Environment, Activities, Information and Communications System, Risk Evaluation, Risk Response), understanding the entity's controls tools is not considered sufficient to test the operational effectiveness of these tools unless there is some automatic operation that helps to ensure consistency in the operation of controls, such as:

- 1- Consistency in applying pre-determined designated duty and performing complex calculations when processing large amounts of transactions or data
- 2- Improving the timeliness of dissemination of release information, providing its accuracy, and facilitating additional analysis of that information
- 3- Enhancing the ability to monitor the performance of the organization's activities, policies and procedures and reducing the risk of fraud control tools. Enhancing the ability to achieve effective segregation of duties by implementing security control tools in applications, databases and operating systems (IFAC, 2023:236).

2-2: Electronic Accounting Information System

2-2-1: Define the Electronic Accounting Information System

Many researchers and writers have provided a set of definitions for the Electronic Accounting

Information System, such as:

“A group of interconnected systems that transform financial events and operations that occurred during a certain period into information that can be used in the decision-making process and determine the financial and economic situation of the organization by using the electronic computer” (Romney & Steinbart, 2009:6).

It has also been defined as “a single set of hardware, software, databases, communications, and procedures configured to collect, store, process, and transform data into information” (Reynolds & Stair, 2010:11)

It has also been defined by “Amidu” as “a term used to describe the accounting system that relies on computer technology to maintain and process financial data in organizations” (Amidu, et al, 2011: 146).

It has also been defined by “Sugut” as a “computer-based software application used to input, process, store, and output accounting information. This application is a support for advanced technology that enables economic units to use computer programs to perform tasks that were previously performed manually” (Sugut, 2012: 2)

It has also been defined by “Neser” as a “a computer-based method for tracking accounting activity in conjunction with information technology resources” (Neser, 2018: 182). It has also been defined by “Bourgeois” as “a set of hardware, software, and communications networks that people build and use to collect, create, and distribute useful data, usually in a plain format.” (Bourgeois, 2019: 11)

It has also been defined by “Ahmed” as “hardware, software, means of remote access, database management, and other information processing techniques used in computer information systems” (Ahmed, 2021: 547). It has also been defined by “Abdul Majid” as “an arrangement of individuals, activities, data, and information technology that work in an integrated manner for the purpose of improving business and assisting management in improving decisions” (Abdul Majid, 2016: 264)

2-2-2 Components of the Electronic Accounting Information System

An Electronic Accounting Information System contains a set of components as follows: (Stair & Reynolds, 2010:12-15, Simkin & et al, 2012: 76, Hardcastle, 2008:16)

A- Equipment: Computers used to perform input activities (input devices include keyboards, mouse, other pointing devices, automated scanning devices, and magnetic ink characters equipment recognition) and processing (processing devices include computer chips that contain the central processing unit (CPU) and core memory) and output (output devices include printers and computer monitors).

Internet: The largest computer network in the world. It consists of thousands of interlinked networks, all of which exchange information freely.

B- Programs: Computer programs that organize the work of the computer.

C- Database: It is a large collection of systematic data that can be accessed by many users and used by many different computer applications. In many large companies, large databases store all the data used by almost every function in the organization electronic data is a collection of texts, drawings, events, images, or other information or data that is represented

in a digital image that is created, saved, indexed, modified, or retrieved by a computer (Michel, 2023: 431)

D- Communications and Networks: Transferring data and information from one computer to another, whether locally or globally, through a set of communication technologies, which results in the emergence of networks and the possibility of transferring data to all parts of the world (Al-Marri, 2023: 1328) Or are the methods concerned with transferring and exchanging ideas between parties in the communication process (Al-Obaidi, 2012: 25).

E- Associates: Who operate the system, including their experience, skills and specialization(Naeem, Yaqoub,2013: 20)

F- Procedures: Strategies, policies, methods and rules for using computer systems, including procedures for computer operation, maintenance and security.

G-Multiple programs, which provides an opportunity to test and differentiate between them as needed (Al-Hiyari, 2022: 453), The variation in organizational structure from one unit to another affects the design of electronic accounting information syst and also affects the way the institution works and its strategy (Al-Dahrawi, 2007: 152)

2-2-3 Objectives of the Electronic Accounting Information System

Using of computers in accounting work can benefit from the following characteristics: (Al-Sharif, 2006: 53)

- 1- The principle of writing data is applied once, where data is entered the first time into the document, and the data in all the files related to it are changed directly at the same time and reports are extracted automatically, which contributes to reducing the effort that accountants expend in carrying out accounting work, as well as accuracy and speed in preparing data at the specified and required time.
- 2- Utilizing the devices and equipment attached to the computer (such as storage, display means, etc.) in the processes of storing, displaying or printing data in various forms and numbers required while maintaining the same efficiency and accuracy. Hence, achieving the objectives of the accounting information system leads to maintaining the confidentiality of the information obtained.
- 3- The electronic accounting information system it helps increase transparency in communicating information to those charged and dealing with the system (Maidani &Obaid, 2023: 26).
- 4- Computing technology has an important role in facilitating the application of international financial reports because it the ease it provides in preparing and preservation of accounting information and the ability of access it at any time and from anywhere that internet service is available (Helio, Abdullah, 2023: 193).
- 5- Purchasing advanced electronic systems in the bank helps achieve the social and environmental dimension (Hamdan, 2020: 4801).
- 6- The use of information technology in all audit levels contributes to collecting and evaluating evidentiary evidence to determine whether electronic systems contribute to protecting the organization's assets, ensuring the integrity of its data, and achieving its objectives efficiently (Al-Ahmedi, AL-Mamour, 2023: 18,). Electronic disclosure of comprehensive income helps improve the quality of accounting information in financial reports (Muhammad, 2023: 18)

- 7- The system fulfills the internal control conditions to protect the project's assets and raise the efficiency of its performance from by providing means of control of the system (Fouda, Shawqi Al-Sayed).
- 8- Electronic management contributes to achieving a radical transformation in the concepts, methods, theories, organizational structures, procedures and legal legislation on which traditional management depends (Fora et al., 2023: 980), In addition to the advantages of sovereignty and transparency that can be obtained using electronic systems, where users identify themselves and maintain control over the storage and management of personal data (Abdel Hamid, 2023: 10)

Third Segment: Evaluation of the Internal Control According to the Framework of the Committee of Sponsoring Organizations (COSO) and the Electronic Accounting Information System

3-1 Research Sample Form

The General Directorate of Education of Baghdad, Al-Karkh, Third, is one of the directorates of the Ministry of Education, which was separated from the General Directorate of Education, Al-Karkh, First, in the year 2006. It has a major impact on the economic and service aspects. As for the affiliated and associated areas that benefit from these services, they were limited to the Taji, Al-Tarmiya, Al-Shuala, and Al-Kadhimiya sectors.

3-2 Evaluation of Internal Control According to the Framework of the Committee of Sponsoring Organizations (COSO)

After reviewing the government unit as a sample of the research and studying the accounting system of the Salaries Division and identifying the most important risks to which those systems were exposed, a proposed survey questionnaire was developed for the internal control components of electronic accounting information systems according to the internal control components of the framework of the Committee of Sponsoring Organizations (COSO) for government units. A set of questions were set to be answer with yeas or no. The internal control was evaluated and the level of internal control risk was determined for each component of the framework, as described below:

Then determine the degree of risk for each component of internal control according to the framework of the Committee of Sponsoring Organizations (COSO) in light of the use of automated accounting information systems for government units, as shown in the equation below:

1- The effectiveness of internal control and determining the level of risk.

Total of Yes or No

* Internal control effectiveness degree = ----- × 100

Total questions

Control risk level = 100 - Internal control effectiveness degree *

In order to apply the previous equations to each component by substituting with the previous equation, the final result shown in the table above appears. In order to determine the degree of risk in an accounting information system for each component of the framework. The degree of risks is as follow:

Low: 0-49

Medium: 50-79

High: 80-100

3-2-1: Control Environment

No.	Question	Answer	
		Yes	No
1	Are there specific codes of conduct and ethical standards that employees must follow?		✓
2	Is there a delegation of authority and responsibilities regarding approval of the purchase and development of electronic systems?	✓	
3	Does the government unit have an organizational structure for e-governance that clarifies the responsibilities of management and software users, delegating of authority, and determining job description for software users to introduce them with the tasks and responsibilities assigned to them?		✓
4	Is there a funding or Automated plan (grants, loan, or other entity) to obtain funds to operate and support the continuation of the use of the system?		✓
5	Does management, body charged with governance, adhere to the recommendations contained in the internal and external auditor's reports?		✓
6	Are all relevant government units been involved in the automation process?		✓
7	Is an appropriate structure been established to operate the program in accordance with the activity of the government unit and the complexity of its activity?		✓
8	With the regard to use of information technology and the resources allocated to it, does the government unit have a sufficient number of employees with appropriate qualifications?		✓
9	Are training courses been held to introduce the use of the system and involve all government unit employees related to the automation process in courses related to the system used?		✓
10	Are legislation, legal and contractual requirements clearly defined, and is the organization's approach to meeting those requirements clearly defined, documented and updated?		✓
11	Is the electronic information system used consistent with the strategy of the government unit being audited?		✓
	Total	1	11

The internal control system is ineffective due to the high degree of risk (91%).

3-2-2 Risk Evaluation

No.	Question	Answer	
		Yes	No
1	Is there a specialized department in the government unit that works on risk management?		✓
2	Has unit management identified and analyzed risks to decide how to manage those risks?		✓

No.	Question	Answer	
		Yes	No
3	Has the government unit identified the types of controlled risks, which are (incorrect entry, failure to use effective passwords, failure to update the encryption system, data theft or loss), and uncontrollable such as natural disasters such as floods and fires. Are there actual measures to reduce the gap in uncontrollable risks management?		✓
4	Have information security policies been defined and approved by management?		✓
5	Were there been plans to review information security policies in the event of significant changes to ensure its continuity, suitability, adequacy and effectiveness?		✓
6	Have all information security responsibilities been defined and assigned?		✓
	Has there been reliance on systems or programs that process data accurately or process accurate data, or both?		✓
7	Are conflicting duties and responsibility not separate from each other and maximize opportunities for authorized adjustment and non-misuse of the organization's assets?	✓	
8	Were the systems obtained by an accredited body?	✓	
9	Are users and others provided with access to network and business services that they have not been specifically authorized to use?	✓	
10	Is a formal user registration and deregistration process implemented to determine access rights?	✓	
11	Are the user's access rights removed upon termination of their contract, or agreement, or modified upon change?		✓
12	Has a policy been developed and implemented to use encryption controls to protect information, such as seizing encryption keys and protecting it? Have these controls been used according to applicable agreements, legislation and regulations?		✓
13	Has the security environment been identified by equipping the building with surveillance cameras and using it to protect areas containing critical information in all information processing facilities to reduce risks resulting from threats, environmental risks, and opportunities for unauthorized access?		✓
14	Have controls been put in place, such as the use of identification cards in server rooms or the use of fingerprint or iris devices to ensure that only authorized individuals are allowed to enter those rooms?		✓
15	Is access to the shared database restricted to one person?		✓
16	Do IT employees have access privileges beyond those required to perform their assigned tasks?		✓
17	Is there an appropriate audit trail, whether paper or electronic, to protect transactions data from loss?	✓	
18	Have audit trail been properly maintained and protected from loss, damage, forgery and unauthorized access in accordance with legislative, regulatory and contractual requirements?		✓
19	By studying the outputs, are there cases of compliance with regulatory requirements and accounting policy followed by government units, such as compliance with tax deductions?		✓
20	Is the equipment protected from power outages and other disturbances caused by failures of supporting facilities?		✓

No.	Question	Answer	
		Yes	No
21	Are power and communications cables carrying data or information services protected from interception, interference or damage?		✓
22	Is the equipment properly maintained to ensure its continued availability and safety?		✓
23	Has equipment, information, or software been moved off-site without prior permission?		✓
24	Has security been applied to assets outside the organization taking into account various risks?		✓
25	Has sensitive software licensed for overwriting been securely verified before disposal or reuse?		✓
26	Do users realize that the equipment has appropriate protection?		✓
27	Detection, prevention and recovery controls to protect against harmful software along with appropriate user awareness?		✓
28	Have planning requirements for audit activities that include verification of operating systems been carefully planned?		✓
29	Are security events reported through appropriate management channels and responded to in accordance with certified procedures?		✓
30	Have responsibilities and procedures been defined to ensure rapid response to information security events?		✓
31	Has a plan been developed by the management regarding recovery from disasters, whether natural or unnatural?		✓
32	Does management periodically confirm the risks position of the program and how this affects the risk profile of the government unit?		✓
33	Is there tight control over files to prevent them from being changed or lost?		✓
34	Have necessary precautions been used to keep the system running, such as backups, specific software, or other emergency procedures?		✓
Total		5	29

The internal control system is ineffective due to the high degree of risk (15%).

3-2-3: Information and Communications

No.	Question	Answer	
		Yes	No
1	Have systems been defined to collect information from internal and external data sources?	✓	
2	Is there a process in place for communicating information to enable all employees to understand and implement internal control responsibilities?		✓
3	Have channels of communication for reporting violations been provided that are ready and fail-safe?		✓
4	Is continuous communication between internal audit and department management regarding risks taken into consideration? Is there mechanism to response to risks in the right moment?		✓
5	Does the method of communication take into consideration the timing and nature of the information?		✓
6	Is relevant information transmitted in a timely manner to third parties, local financial institutions and other external parties?		✓
7	Have you been in contact with professional associations or private security apparatuses?		✓
8	Do the information systems used by the unit process and covert data into appropriate information?		✓

9	Are records used by the user to record events and errors for review when needed?	✓
10	Does the information obtained achieve the objectives of the governmental unit?	✓
11	Were the elements of an appropriate information system used to obtain good results, such as identifying information, obtaining information, processing information, reporting information, and selecting qualified employees to operate the system and inform them of its importance?	✓
Total		1 10

The internal control system is ineffective due to the high degree of risk (91%).

3-2-4 Control Activities

No.	Question	Answer	
		Yes	No
1	Is there a separation between the tasks of analyst, programmer and operator?	✓	
2	Are there official approvals to use the program based on a contract concluded between the donor and the beneficiary?		✓
3	Have the contracting parties been informed of all the conditions concluded in the contract, with the signatures of both parties placed on the copies of the contract?		✓
4	Is there documentation of the programs and changes that occur?		✓
5	Are there official approvals for using the program?	✓	
6	Have the identities of final users and system operators been identified and verified?		✓
7	Were the secret codes used to enter the system managed in a non-interactive manner and the password was not ensured by using words containing a mixture of alphabets, special numbers and symbols that are difficult to detect even by IT experts or by another user by conducting experiments or by writing symbols?	✓	
8	Is there regular system maintenance and system checking, and are precautions used to keep the system running, such as backups, specific programs, or other emergency procedures?		✓
9	Does the program include automatic updates?		✓
10	Is the electronic system flexible enough to make changes whenever necessary?		✓
11	Are there devices to protect the operational range?		✓
12	Has the system been linked with all relevant departments to ensure that central distribution of data and the delivery of information the various relevant departments?		✓
13	Are there backup files to recover data and take backup copies of information, programs and images of the system that are tested periodically in accordance with the agreed upon backup policy?		✓
14	Are the system users experienced and qualified?		✓
15	Have the necessary supplies been provided to operate the system (purchasing computers or servers)?		✓
16	Does implementing the system support the activity of the government unit under audit and make it more efficient than it was before using that system and the possibility of obtaining future improvements?		✓
17	Have specialized committees been formed to direct the program at the management level?		✓
18	Have alternatives been developed for the process of implementing the electronic system in the event of failure to achieve the objectives of accounting information systems through the use of that system?		✓
19	Does management evaluate the impact of use of the software on the financial and organizational requirements of the government unit being audited?		✓
20	Does management establish best practice rules for the use and placement of the software?		✓
21	Is the data entered into the program officially approved by the management?	✓	
22	Is the data entered into the program correct and complete?	✓	
23	When used, does the system include commands that prevent the duplication or omission of recording transactions?		✓
24	Does it include orders preventing the processing of incomplete transactions, such as recording the number and date of the document, the entity, and the name of the person who owns the document?		✓
25	Is data been entered and verified on each application?	✓	
26	Is the process limited to authorized operations only?	✓	

No.	Question	Answer	
		Yes	No
27	Have the system's electronic operating outputs been verified as accurate and complete?		✓
28	Have the outputs been distributed to authorized persons?	✓	
29	Are the system outputs audited by independent people?	✓	
30	Has the database been accessed by unauthorized persons without adhering to the access control policy?	✓	
31	Is access to the software source code been restricted?		✓
32	Has the use of other programs capable of override the system been restricted?		✓
33	Is there tight control over files to prevent them from being changed or lost?		✓
34	Are all rooms and facilities used by the system secure?		✓
35	Has physical protection against natural disasters, malicious attacks or accidents been established and implemented?		✓
36	Are operating procedures documented and available to all users who need them?		✓
37	Is a supporting security policy and measures adopted to manage resulting from the use of mobile devices?		✓
38	Is a supportive security policy and measures implemented to protect information accessed, processed and stored in remote work sites?		✓
39	Has an access control policy been developed, documented and reviewed based on information security and business requirements?		✓
40	Is changes in the organization affecting information security controlled?		✓
41	Have resources been utilized and adjusted for future expansion to ensure the desired system performance?		✓
42	Are data related to development, testing and operational applied separately?		✓
Total		10	32

The effectiveness of the control system is medium due to it achieving a risk score of 76%.

3-2-5 Monitoring Activities

No.	Question	Answer	
		Yes	No
1	Does the government unit have an audit program covering the software processes used?		✓
2	Does the government unit have a specific work plan that is followed up periodically?		✓
3	Are deficiencies in internal control evaluated by the government unit and communicated to relevant parties in a timely manner in order to take appropriate decisions?		✓
4	Are business requirements updated periodically to accommodate updates resulting from the use of new software?		✓
5	Does the management monitoring the extent of compliance with the regulations and instructions issued by it?		✓
6	Does the Internal Audit Department follow up on management recommendations and act on them?		✓
7	Are the controls established by management regarding operations and control processes ensured that they are effective?		✓
8	Is compliance with what is issued by the regulatory and supervisory authorities, the Board of Directors and senior management, and reports on that periodically?		✓
9	Are the system's outputs monitored, verified and delivered to relevant authorities?	✓	
10	Has the errors in the system outputs been identified and corrected?	✓	
Total		2	8

The internal control system is ineffective due to the high degree of risk (80%)

After obtaining the answers, a value of (1) is given for each answer to facilitate the process of applying the equations for measuring the degree of effectiveness of internal control and determining the final risk ratios for each component, as shown in the table below:

No.	component	Total number of questions	Total sum of yes	Total sum of No	Final score for risk level %
1	Control Environment	11	1	10	91
2	Risk Evaluation	34	5	29	85
3	Information and Communication	11	1	10	91
4	Control Activities	42	10	32	76
5	Monitoring Activities	10	2	8	80
	Total	108	19	89	82

Conclusions

1- The results of the evaluation of the internal control system according to the components of framework of the Committee of Sponsoring Organizations (COSO) for government units subject to electronic operation using an automated accounting system for the salaries clause of the governmental unit in the research sample showed the following percentages according to each component of the framework, as shown below:

A- Control Environment Components

Ineffective: This is due to the high percentage of final risk achieved by this component, which reaches 91%, for the reasons explained below:

- 1- Lack of a list of professional conduct and ethical standards that must be followed by employees.
- 2- The lack of an organizational structure for electronic governance and the lack of a job description that define the responsibilities and powers of employees and users of the automated accounting information system.
- 3- Failure to hold training courses for employees who use the electronic system that are appropriate to the nature of the system used.
- 4- Failure to clearly define, document and update legal and contractual legislation and the organization's approach to complying with these requirements.

B- Risk Evaluation

Ineffective: This is due to the high percentage of final risk achieved by this component, which reaches 85%, for the reasons explained below:

- 1- The lack of a specialized department in the government unit that works on risk management, and there is no continuous communication between the internal audit department and the government unit management regarding risks and the lack of a mechanism to respond to risks in a timely manner.
- 2- Lack of attention to the security aspect of the electronic information system in terms of dealing with approved security agencies to ensure the continuity, suitability, efficiency and effectiveness of that system for the government unit.
- 3- Manual intervention in the process of processing or modifying the system's outputs as a result of a flaw in the design of the electronic accounting information system.

C- Information and Communications components

Ineffective: This is due to the high percentage of final risk achieved by this component, which

reaches 91%, for the reasons explained below:

- 1- Failure to provide ready and automated communication channels for reporting violations against malfunctions.
- 2- Failure to establish information communication processes to enable all employees to understand and implement internal control responsibilities.
- 3- Do not use logs to record events and errors and review them when needed by the automated system users.
- 4- The electronic accounting information system did not achieve the goals of the government unit desired by using that system in terms of accuracy and speed.
- 5- The lack of minutes of meetings to exchange information between officials and system operators and to fix weak points in the system outputs by system employees or operators.

D- Control Activities

Medium effectiveness: This is due to the high percentage of final risk achieved by this component, which reaches 77%, for the reasons explained below:

- 1- Lack of documentation of programs and changes that occur.
- 2- Lack of adequate maintenance to keep the system running.
- 3- The system is not linked with all relevant departments to obtain data and communicate information centrally.

E- Monitoring Activities

Ineffective: This is due to the high percentage of final risk achieved by this component, which reaches 80%, for the reasons explained below:

- 1- Lack of an action plan to address deviations and follow them up periodically and address them.
- 2- Failure to evaluate deficiencies in internal control and report them in a timely manner to the relevant authorities.
- 3- Failure to make updates to work requirements that are commensurate with the updates resulting from the use of new programs.
- 4- Lack of - Monitoring Activities by internal audit regarding management recommendations and acting accordingly.

Second: The failure of the Federal Financial Supervisory Authority in the government unit of the research sample to evaluate the internal control system according to the components of framework of the Committee of Sponsoring Organizations (COSO) regarding the unit's work under electronic operation and its use of an automated accounting information system.

Recommendations

First: We recommend the necessity of addressing the risks resulting from the use of the automated accounting information system for each component of the framework and working to reduce them to an acceptable level, as shown below:

A- Control Environment Component

Developing a list of rules of professional conduct and ethical standards, in addition to developing the organizational structure for electronic governance, determining a job description to define the

responsibilities and powers of employees and users of the automated accounting information system, and the management selects the operators and programmers with specialization, competence, and skill in operating and using electronic programs and working to align the use of the system with the strategy of the government unit using the program.

B- Risk Evaluation

Establishing a specialized department in the unit to work on risk management and achieving continuous communication between the internal audit department and the management to identify the causes of the risks occurring and develop an appropriate mechanism to respond in a timely manner. In addition to paying attention to the security aspect of protecting programs from malfunctions, ensuring business continuity, and seeking the help of competent designers to design programs according to the unit's requirements, to prevent program penetration and the occurrence of manual intervention that may cause messing with the system outputs of that unit.

C- Communications and Information Component

Providing ready and automated communication channels for reporting violations against malfunctions and enabling all employees to understand and implement internal control responsibilities and using records to record these events and malfunctions and review them when needed by automated system users.

D- Control Activities Component

Defining the function of the analyst, programmer, and operator of the system, separating conflicting functions, in addition to documenting the programs and the changes that occur, forming efficient committees to maintain the programs and inspecting them periodically, and linking the system with all relevant departments to obtain data quickly, when needed, delivering information in a timely manner, and ensuring it is delivered in the correct form and direction.

E- Monitoring Activities Component

Evaluate shortcomings in internal control and report them to the relevant authorities, create an action plan to address deviations and Monitoring periodically, emphasize the need for the internal audit department to Monitoring on management recommendations and the need to make updates to the program and use advanced programs resulting from the use of new programs.

2- We would like to recommend that the Federal Financial Supervisory Authority in the government unit should evaluate the internal control system according to the framework of the Committee of Sponsoring Organization (COSO), determine the causes of shortcomings, record them in their reports as notes, and Monitoring with the management to address the cases that led to a low level of internal control.

References

- 1- Romney, Marshall & Paul John Steinbart, (2009.), " Accounting Information Systems " 9th International Edition, Prentice Hall.
- 2- Simkin, Mark, Jacob M. Rose Carolyn Strand Norman, (2012) " CORE CONCEPTS OF Accounting Information Systems", Twelfth Edition, JOHN WILEY & SONS, INC.
- 3-Hardcastle, Elizabeth, (2008), "Business Information System"
- 4- Sugut, Olive Chpkorir, (2012)," The Effect of Computerized Accounting Systems on The

- Quality of Financial Reports of Non-Governmental ", Organizations in Nairobi County, Kenya.
- 5- Nesar, Ahmed Giuma Omar, Nassar, Mohamed Giuma, (2018), " The Role of Electronic Accounting Information Systems in the Quality of Accounting System Outcomes ", International Journal of Scientific and Research Publications, Volume 8, Issue 12, December 2018
 - 6- Piazza. L. Michael, (2014), Quick Reference Guide, Committee of Sponsoring Organizations (COSO) Internal Control Integrated Framework.
 - 7- Amidu ,Mohammed & eta, (2011) " E-Accounting Practices among Small and Medium Enterprises in Ghana".
 - 8- Reynolds, George, Stair, Ralph, (2010)"principles of Information System" A managerial Approach, 9Ed.
 - 9- Al-Gabali, Samir Abdel Azim, 2022, "The impact of integration into the dimensions of COBIT 5 and internal control components according to the COSO framework in reducing cloud accounting risks" - a field guide in Egyptian telecommunications companies, Alexandria Journal of Accounting Research / Accounting and Auditing Department / Third Issue - Volume 22.
 - 10- International Auditing Practice Statement (IAPS) 1013, (2002) "Electronic Commerce— Effect on the Audit of Financial Statements" should be read in the context of the "Preface to the International Standards on Quality Control, Auditing, Review, Other Assurance and Related Services," which sets out the application and authority of IAPSs.
 - 11- International Federation of Accounting, IFAC, (2023), ISA 315 (Revised) Identifying and Assessing the Risks of Material Misstatement.
 - 12- International Federation of Accounting, IFAC,(2023), ISAE 3402 Assurance Reports on Controls a at Service Organization
 - 13- Hamdan, Khawla Hussein, (2020)," Performance Evaluating of Islamic banks in achieving sustainable development Applied research in the Iraqi Islamic Investment Bank and the Development", International Journal of Psychosocial Rehabilitation, Vol. 24.
 - 14-Bediwi, Akram Khashea, Sabri, Bassam Ameen, Shanshool, Mohammed Hayder Mohammed, (2022) "The Effect of Internal Control in Supporting the Implementation of Cost Techniques in Iraqi Companies", Social Science Journal, vol.12, n^o2.
 - 15- Hamdan, Khawla Hussein, (2022) "Evaluating the Internal Control of Disaster Management According to Sendai Framework for Disaster Risk Reduction (SF-DRR) In Iraq ", SPECIALUSIS UGDYMAS / SPECIAL EDUCATION 20--X (YY).
 - 16- Yousif, Najat Saleem, Mohammed, Safaa Ahmed, "The Role of Internal Auditing in Governance of, Science Journal, vol.12, n^o2.
 - 17- Helio, Mustafa Mohamed, Abdullah, Bushra Najim, (2023)" The Effect of Cloud Computing in Facing the Challenges of Applying IFRSs in Iraqi Private Banks", International Journal of Research in Social Sciences and Humanities, Vol. No. 13.
 - 18- Al-Tai,Bushra Mahdi Saleh, Muhammad, Iman Shaker, "Internal banking supervision requirements and their impact on the development of electronic accounting information systems applied research in a sample of Iraqi private banks" ,(2017), Journal of Accounting and Financial Studies, Volume Twelve, Issue 40, Third Semester.
 - 19- Aljboul, Moyasser Menazel, Abdel Megid, Narmeen Youssef,(2023)," The role of the external auditor in reviewing internal control in electronic accounting systems/Applied research", Journal of Accounting and Financial Studies, Volume.18,ISS.62.
 - 20- Fattah, Ibtisam Ahmed, Mohammed, Raja Jassim, (2012), " Evaluating the internal control

- system in the General Company for Battery Manufacturing", A field study in the General Company for Battery Manufacturing, Journal of Accounting and Financial Studies - Volume Seven - Issue 20 - Chapter Three.
- 21- Hussein, Enas Muhammad Ali, Muhammad, Mahmoud Ismail, (2018), "The effective role of computer information systems in the tax assessment processm, Journal of Accounting and Financial Studies, Special issue, First International Scientific Conference.
 - 22- Al-Sharida, Nadia Abdel-Jabbar Muhammad, Al-Samarrai, Ammar Essam Abdel Rahman, (2021), " The role of the use of automated accounting systems technology in enhancing the efficiency and effectiveness of the internal control system", Volume 16, special issue, The Second International Scientific Conference and fourth national.
 - 23- Al-Ahmedi, Ali Mohammed, Nayef, Al-Mamouri, Ali Mohammed Thijeel, (2023)," A proposed audit program for a comprehensive electronic banking system based on business risks"(applied research).
 - 24- Al-Ahmedi, Ali Mohammed, Nayef, AL-Mamouri, Ali Mohammed Thijeel, (2023)," Auditing the comprehensive electronic banking system to detect operational business risks", (applied research) .
 - 25- Al-Sharif, Hurria Shaaban, "The Risks of Electronic Accounting Information Systems," "An Applied Study on Banks Operating in the Gaza Strip, a Master's Thesis in Accounting and Finance from the Faculty of Commerce at the Islamic University of Gaza, 2006.
 - 26-Rifa'a, Thamer Mazid, 2017, "Principles of Auditing", Dar Al-Manhaj for Publishing and Distribution, Amman, Jordan.
 - 27-Abdel Majid, Bourkeeb Muhammad, 2016 , "Requirements for auditing electronic accounting information systems in light of international standards," New Economy Journal, Issue 12 - Volume 1.
 - 28-Al-Hiyari, Muhammad Musa Odeh, (2022), "Electronic accounting and its relationship to accounting information systems,"Arab Journal for Scientific Publishing (AJSP) ISSN: 2663-5798.
 - 29-Nasima, Mahiot, (2019-2020), "Study of the impact of establishing the conceptual framework of the internal control system according to the COSO structure on the organization's performance." Economics", PhD thesis, University of Algiers 3College of Economics, Commercial Sciences and Management Sciences.
 - 30- Al-Ramahi, Zarhi, 2023, "Modern trends in internal auditing according to international standards," Chapter Three.
 - 31- Robertson, Jack, Timothy, Louwers, (2002),"Auditing and Assurance Servis", 16 Ed, Lrwin.
 - 32- Al-Tamimi, Abbas Hamid, Haddab, Fatima Faza, 2018, "Evaluating the internal control system in non-governmental organizations", Applied research in the Iraqi National Olympic Committee, Journal of Accounting and Financial Studies, Volume Thirteen, Issue 42, First Semester of 2018.
 - 33- Al-Basha, Adel Sobhi Abdel Qader, 2023, "Obstacles to modernizing internal control systems under the updated COSO framework in the local environment." Applied study at the College of Administration and Economics - Iraqi University, Journal of Administration and Economics Vol. (special issue) 2023 ISSN P.2221-5794 ISSN E.2790-2910>
 - 34- Muhammad, Safaa Ahmed, Abdul Karim, Nawar Ali, 2020, "The extent of Iraqi oil companies' commitment to implementing internal control procedures according to the updated COSO framework," an applied study in the Central Oil Company Journal of Economics and Administrative Sciences Vol.26 (NO. 124) 2020, pp. 529-548.

- 35- Yassin, Vian Abdul Rahman & Mansour, Rahim Mansour, 2022, "A proposed model for a checklist and evaluation of the internal control system according to the framework of a committee Supporting Organizations (COSO)," Kirkuk University Journal of Administrative and Economic Sciences, Volume (12), Issue (2).
- 36- Al-Ramahi, Nazal Mahmoud, 2016, Measuring the extent of application of the (COSO) framework for internal control from the point of view External auditors in public joint stock companies listed on the Stock Exchange Amman, Al-Zarqa Journal for Humanitarian Research and Studies - Volume Seventeen - Issue Two, 2.
- 37- Naeem, Ali Hamid, Yaqoub, Faihaa Abdullah, 2013, "A proposed guide for auditing the internal control system according to the COBIT framework", applied research in the General Company for Petra Industries.
- 38- Fouda, Shawqi & Al-Sayed, Sayed Sayed Abdel Fattah, 2019, "The Impact of the Efficiency and Effectiveness of Electronic Accounting Information Systems" "On Improving Performance Evaluation in Commercial Banks with a Field Study," Journal of Contemporary Business Studies, Issue Six.
- 39- Thabet, Thabet Hassan, Chanshul, Muhammad Haider Muhammad, 2022, "The role of applying the internal control system structure according to the COSO framework in reducing risks." "Electronic Banking", Journal of Financial and Accounting Sciences - ISSN 2709-2852 - Special Issue of the Banking Sector Conference - Challenges of Reform and Development.
- 40- Elias, Ben Ali, 2017, "The extent of responsiveness of the internal control system in institutions Economic with coso frame Case study of the Oasis Mills Corporation, a memorandum submitted to complete the requirements for the Mast Academy certificate, second phase In the field: economics, management and commercial sciences Branch of Financial and Accounting Sciences Specialization in in-depth accounting and fiscal studies.
- 40- Fatih, Briha, 2016, "The extent to which the internal control system in Algerian institutions is compatible with the perspective of the American Institutional Sponsoring Organization COSO ", (Committee Of Sponsoring Organization) Case study of "Bayat Catering).
- 41- Al-Ghanoudi, Issa Abdullah, 2020, "The Possibility of Adopting the COSO Framework for Internal Control of Jumhouria Bank," An Applied Study in the Branches of Jumah Bank.
- 42- Al-Obaidi, Fatima Naji, 2012, "The Risks of Using Computerized Information Systems and Their Impact on the Effectiveness of the Auditing Process in Jordan," Master's Thesis, Department of Accounting, College of Business, Middle East University.
- 43- Faura, Muhammad Nahed, Hashem, Osama Yahya, Abdel Aziz, Sumaya, Sharum, Qamrina, Abu Shawish, Abdul Karim, 2023, "The impact of electronic management requirements on improving the quality of academic service at Al-Aqsa University in Gaza - Palestine.", e-ISSN: 2805-4741 , <http://iecons.usim.edu.my>
- 44- Midani, Mohammed Atef, Obaid, Shaher Mohammed, 2023, "The Role of Tax Governance as a Mediating Variable Between Information Systems and the Reduction of Tax Evasion at the Income Tax Department in the West Bank - From the Viewpoint of its Employees ", Journal of Al-Quds Open University for Administrative & Economic Research & Studies Vol. (8) No -)20(.November 2023 <https://journals.qou.edu/index.php/eqtsadia> E-ISSN: 2410-3349/ P-ISSN: 2313-7592
- 45- Michel, George Nabil, 2023, "The Authority of Electronic Commercial Books in Evidence in the Saudi System," Al-Azhar University, Journal of Jurisprudential and Legal Research, Issue Forty
- 46- Abdel Hamid, Rania Sultan Muhammad, 2023, " The Effect of Using Blockchain Technology on The Accounting Environment in Egypt (Field Theoretical study) ", Egyptian Journal of Commercial Studies, Volume 47, pages 227-262.

- 47- Muhammad, Muhammad Khalifa Issa, 2023, "Repercussions of electronic disclosure via digital platforms regarding items Other Comprehensive Income on Rationalizing Investors' Decisions", *Scientific Journal of Financial and Administrative Studies and Research*, Volume (Fifteen), Special Issue.
- 48- Arens, Alvin & Elder, Randal & Beasley, Mark, 2012, "Auditing and Assurance Services", Pearson Education, Inc.
- 49- Elias, Ben Ali, 2017, "The extent to which the internal control system in economic institutions responds to the COSO framework," case study of "Oasis Mills Corporation," Master's thesis from the Second Matar Academy, economics, management, and commercial sciences, branches of financial and accounting sciences, specialization in accounting and fiscal studies. In-depth, Kasdi-Merbah University – Ouargla.
- 49- Al-Marri, Rashid Muhammad, 2023, "The Impact of Information Technology on the Information System and Internal Control," *Al-Azhar University - Faculty of Sharia and Law in Damanhour, Journal of Jurisprudential and Legal Research*, No. 40.
- 50- Al-Dahrai, Kamal El-Din Mustafa, 2007, "Accounting Information Systems in Light of Information Technology", Alexandria - Egypt, New University Publishing House
- 51- Stedman, J. M., Spalding, T. L., Gagné, C. L., & Hancock, C. L. (2023). The Relationship of Concepts, Memory, and Language in the Cognitive Psychology of Thinking: An Aristotelian–Thomistic Appraisal. *The Journal of Mind and Behavior*, 44(1/2), 15-36.