

# The Role of Internal Auditors in Reducing Audit Risks Associated with Electronic Accounting Information Systems in Libya

Shamsaaddeen Faraj\*, Issedeeq Saadi

Department of Accounting, Gharyan Accounting Faculty, Gharyan University, Libya

Received September 18, 2024; Revised January 8, 2025; Accepted February 18, 2025

## Cite This Paper in the Following Citation Styles

(a): [1] Shamsaaddeen Faraj, Issedeeq Saadi, "The Role of Internal Auditors in Reducing Audit Risks Associated with Electronic Accounting Information Systems in Libya," *Universal Journal of Accounting and Finance*, Vol. 13, No. 2, pp. 69 - 80, 2025. DOI: 10.13189/ujaf.2025.130203.

(b): Shamsaaddeen Faraj, Issedeeq Saadi (2025). *The Role of Internal Auditors in Reducing Audit Risks Associated with Electronic Accounting Information Systems in Libya*. *Universal Journal of Accounting and Finance*, 13(2), 69 - 80. DOI: 10.13189/ujaf.2025.130203.

Copyright©2025 by authors, all rights reserved. Authors agree that this article remains permanently open access under the terms of the Creative Commons Attribution License 4.0 International License

**Abstract** This study investigates whether internal auditors in Libyan oil companies possess the necessary competence and capabilities in the security of electronic accounting information systems within an era of transition from manual auditing to electronic accounting information system auditing. The study<sup>1</sup> also examines the issue of whether internal auditors implement sufficient safeguards to address the risks associated with electronic accounting information systems. A questionnaire survey adopted for data collection revealed that: internal auditors in the sampled companies possess a high level of competence and efficiency in electronic accounting information system security; and that they also follow all protective measures to counter the risks of electronic accounting information systems. However, descriptive statistics show that the mean scores of participants' responses regarding the competence and efficiency of internal auditors in electronic accounting information system security were lower than the overall mean of the axis. This could be seen as a deficiency on the part of internal auditors in reviewing risks related to electronic accounting information systems, monitoring management's implementation of regular maintenance of electronic systems, ensuring the existence of sufficient protection programs to scan electronic

programs or magnetic disks, implementing procedures to limit risks arising from electronic equipment damage, and periodically evaluating information security applications within the company. Descriptive statistics also indicate that the average scores of participants' responses regarding internal auditors' adherence to all protective measures to counter the risks of electronic accounting information systems were lower than the overall mean of the axis. This could be seen as a deficiency on the part of internal auditors in monitoring IT staff in implementing required security measures, participating in updating security methods according to changes in the evolving IT environment, participating in developing specific security policies such as selecting the appropriate technology and its effectiveness, participating in developing and formulating a strategy for developing the security of electronic accounting information systems, and contributing to the detection of security breaches through reports and describing the type of breach.

**Keywords** Role of Internal Audit, Reducing Risks, Electronic Accounting Information Systems, Libya Oil Companies

---

<sup>1</sup>This article has been translated from its original Arabic version [21] to English in order to ensure its widespread accessibility and in acknowledgement of the fact that IT language is in English and the audit profession is moving towards total integration with IT capabilities and indeed to Artificial Intelligence (AI).

## 1. Introduction

The rapid advancements in information and communication technology and the increasing competition among businesses in the utilization of information technology (IT) have led to significant changes in various fields at all levels. Accounting is one of the most impacted areas, as the current period has witnessed a rapid shift towards the use of electronic accounting information systems (EAISs). This shift from the manual audit system to the electronic audit has become an urgent necessity for the advancement of the audit profession, which has entered the era of IT [1,2,3].

In the Libyan context, we observe a transition from manual to EAISs in many sectors and institutions, especially the oil sector<sup>2</sup>, which is characterized by its speed, accuracy, and diversity of applications and business transactions. However, this technological progress has not been accompanied by a similar development in the capabilities and competencies of the users of the technology, or in the control procedures and measures, thereby promoting the emergence of risks that limit the effectiveness of using EAISs. In this regard, the Director of Internal Audit of the NOC emphasized the importance of transitioning from the current methods and approaches of internal auditing to more modern and advanced ones that keep pace with the latest developments in this field [4]. A review of the associated literature is presented in the next section, which is followed by Section 3 and its sub-sections detailing the research methodology. Section 4 presents the data analysis, and Section 5 reports the findings and a discussion of these. Finally, Section 6 concludes the paper and offers recommendations.

## 2. Literature Review

In exploring the accounting literature, the aim is to identify the risks associated with EAISs as a means of developing a suitable theoretical framework for the empirical study to follow. Specifically, the role of Internal Auditing in mitigating these risks is important in this connection, as is the need to understand the necessary protective measures to prevent or reduce the occurrence of such risks. The most significant risks facing EAISs include the following:

The first can be seen as human resource risks which typically occur during the design of equipment or information systems, programming, data selection or compilation, data entry, or user authorization processes. These risks constitute the vast majority of problems related to the security and safety of information systems within an organization [5]. Despite the precision and high reliability of computers, systems are not immune to risks and errors.

Data is entered into computers by individuals, and the programs that operate the computers are also designed by individuals. Therefore, the human element inevitably exposes the system to risks resulting from incorrect actions or system downtime due to any reason [6]. For instance, a programmer in a banking system was able to modify an interest calculation program to add decimal fractions to his personal account. It was very difficult to detect such manipulation, as the customer was unlikely to complain about a difference of only a few cents in their interest calculation [7].

Secondly, there are the network risks which come with business networks generally whether they be internal or external to the organization. Such risks are difficult to assess because they have many protection requirements at different levels within both the system, and the external services that interact with the system. Protecting computer networks from hacking has also become a complex problem that increases with the advancement of computer technology. Network outages due to equipment failure, data or program loss due to accidents, or other reasons can lead to significant costs and additional expenses. Additionally, network service disruption, which refers to interruptions in network connectivity or services provided to users within the network, can occur through various means, such as sending fake packets that fill memory spaces and prevent the network from continuing to operate, or sabotaging message segmentation information, which can cause the system to fail when trying to reassemble the messages upon arrival. This highlights the importance of promptly identifying and addressing network vulnerabilities, as their persistence can have serious consequences for the quality of the output of EAISs [8]. Moreover, the quality of electronic internal audits in the Jordanian Listed Service Companies is also influenced by top management strategy [9].

The third type of risk is that related to hardware, storage media, and software; damage to hardware, storage media, and software can result from actions within the organization or external influences. For instance, equipment and hardware are exposed to this risk due to technological obsolescence or accidents such as intentional sabotage, rough handling of equipment, theft of components, fluctuations in the electrical current, power outages, or failures of air conditioning or heating systems. In addition, environmental problems surrounding the computer are also considered risks that can physically damage the computer and its equipment. It is common to see water or steam pipes running inside computer rooms, and leakage or explosion from these pipes can lead to significant losses. In many cases, a fire in the fireproof computer room can occur due to a fire in a neighbouring room or on an upper floor [8].

Storage media might be corrupted due to exposure to external radiation. For instance, the literature reports that one centre faced a problem of damage to magnetic tapes,

---

<sup>2</sup> For more details see Appendix 1

the cause of which could not be determined by the centre manager. However, upon observation, it was discovered that the damaged tapes were stored at the bottom of a tape storage cabinet, and that when the vacuum cleaner was polishing the floor, it generated a magnetic field around the tapes located on the bottom shelf of the cabinet. It is, therefore, essential to ensure security levels related to this risk and to provide periodic reports that show levels of security compliance [10].

The fourth risk relates to viruses and malware which have become widespread in the world of computers. These are unauthorized programs that consist of a set of code instructions that can spread within a system during data operation to perform unauthorized tasks without leaving any electronic trace that can be used to detect these programs and evaluate internal control systems. These interventions by others can also be used to thwart the auditor's work by identifying the sudden test processes that the auditor performs without the knowledge of the organization, as the virus deals with them and deceives the organization about the robustness of the control points within its accounting information system [11]. However, viruses can also replicate themselves multiple times in internal or external memory, consuming available storage space and preventing users from utilizing these storage locations for their data and programs. Additionally, some viruses can damage the paths that contain the loading and execution programs that are supposed to reside in the computer's memory when it starts up to provide service to the computer's users. It is, therefore, crucial to promptly update antivirus programs both to prevent the risks that viruses can pose, and to limit their severe impact on outputs of EAISSs.

Fifthly, there are environmental risks to consider. Electronic information systems are exposed to natural threats and disasters (fires, volcanoes, earthquakes, and floods), and environmental threats (electricity, heat, cooling systems, and problems resulting from explosions). For instance, fires can destroy computer equipment and damage programs and data, which may require reconstruction costs greater than the cost of the computer itself. It may take several years for the project to recover its position. Earthquakes, hurricanes, and floods, although rare, are usually destructive and cause severe damage to computer components and software. Interruptions or fluctuations in the electric current lead to incorrect recording in the computer's internal storage due to incorrect reading from the magnetic disk unit [10,12,13]. In this context, the interruption of a supplier's business in general, or the termination of a relationship with one organization by another, and the unavailability of spare parts in the local market, can lead to weeks of lost computer time until these parts are imported. Consequently, there is a need to counter such risks, and this requires an organization to deal with reputable suppliers to ensure continuous communication to guarantee effective

maintenance and updating of all operations [8, 10].

Simultaneously, the role of Internal Auditors (IAs) in mitigating the above-mentioned risks to EAISSs must be considered.

Firstly, in terms of protection against the risks related to human resources, it is seen that many individuals pose a threat to the security of such electronic information systems, and these may be employees within the system or employees in other systems outside that system. These individuals include senior and middle management, systems analysts, programmers, operators, and users. They are potentially threatening because of their unintentional errors when entering data, errors in operating programs, or errors in system specification, as well as intentional errors such as viewing confidential data, deleting files, or confidential documents. Thus, the IA's role in this case is to verify the management's review of the implementation of the necessary protective measures for the security of accounting information systems from human resource risks. Such measures include segregation of duties and responsibilities among individuals, segregation of information among them, job rotation among employees, and continuous monitoring of individuals' behaviours and actions [14].

Secondly, EAISSs require a set of hardware and equipment, and some components of this operate independently while others function within an integrated system. Included are the computer system and its accessories, as well as the environmental system (air conditioning system and electrical power supply system). In general, all the equipment and devices belonging to the EIAS are subject to exploitation in one way or another to collect information about the nature of on-going business in an unauthorized manner or to damage the information being handled through the applications used. Additionally, this hardware and equipment may be exploited negatively, leading to a breach of information security and confidentiality. Variations at the levels of electrical power supplied to the equipment or exposure to heat, humidity, dust, or theft can all lead to damage to the equipment [8].

To provide protection for the security of EAISSs from these risks related to hardware and equipment, a set of measures must be in place to protect the devices and their accessories, as well as both programs and data storage media. The IAs must be familiar with these measures and procedures, should follow up on their implementation by management, and should include in their reports, reference to the extent to which management adheres to the requirements for protecting hardware and equipment, and the policies and procedures put in place to protect their EIASs from the risks associated with hardware and equipment [8].

Thirdly, the viruses are programs that are designed to disrupt and delete data from computer memory encoded such that they spread quickly between connected devices through networks or via the use of disks between different

devices. The damage can be mitigated by using original or licensed software from reputable software companies, creating additional copies of the software and files used, and equipping computers with antivirus software on a continuous basis to ensure the detection of new viruses. The IA's role includes following up on management's implementation of procedures and requirements for protection against the risks of viruses and malware, and ensuring the existence of policies that require the storage of data on special disks, which should not be mixed up. This procedure can mitigate the losses resulting from viruses [15].

Fourthly, the environmental risks (earthquakes, storms, floods, hurricanes, and power outages and fires) among other disasters, which may result in the termination of the organization's operations and the loss of data, must be mitigated as far as possible since restoring and repairing in the aftermath of such disasters can take a long time and incur significant costs. Appropriate insurance policies covering such losses, the creation of backup copies of programs and files, and the development of a contingency plan to address environmental disasters, are all steps that management should take. However the internal auditor has a role in this area, that being to suggest measures that provide protection against these risks and to follow up with management in taking the necessary measures to address these disasters if they occur [12].

Fifth come the numerous risks that accompany a networked world, where reliance on the transfer of information from one place to another over networks is increasing. Those responsible for the design, implementation, and operation of the EAIS must study the risks that the information network may be exposed to, so that the appropriate system for dealing with the variety of risks can be devised. Here also, the role of the IA is to follow up with management in taking and implementing the necessary measures to protect EAISs from network risks [13].

In a study of one Libyan oil company, IAs were seen to play a vital role in identifying the risks of EAISs, specifically monitoring the intentional/unintentional entry of incorrect data by company employees, the introduction of computer viruses into the system, and both natural and unnatural disasters such as power outages and the sharing of the same password by some employees. This indicates the existence of sufficient protective measures in that particular organization [15]. Moreover, the use of electronic accounting systems leads to the development of internal auditing, and provides more accurate, timely, and efficient information than a manual system. The IA function also establishes a system of risk management procedures in the company, monitors and evaluates its effectiveness, and helps in reducing the risks by speedy detection of errors and manipulations in the books and records [16, 17]. All of these measures are fundamental in

the effort to achieve sound corporate governance [18].

Internal Auditors of accounting information systems must be knowledgeable about those systems and the associated risks, as well as the methods and tools necessary to detect, correct, and avoid these risks. Knowledge and understanding of this kind enable them to perform audit tasks and ensure the efficiency and effectiveness of the control procedures used to protect accounting data and information, and other procedures related to the security and protection of data and information within the EAIS. However, despite the recent developments in IT, its use in the field of supervisory work is still on a small scale in terms of its application by economic units at the level of auditing and auditing work, and especially with regard to electronic monitoring programs [19]. Hence, there is a need to identify the competence of IAs in auditing the security of EAISs and the control procedures used to protect accounting data and information in Libyan oil companies

Internal Auditors are facing significant challenges due to the rapid advancements in computer technology and its application in developing accounting and auditing systems within organizations, particularly in the oil industry. These technological advancements have introduced new risks that particularly impact upon IAs, one key challenge being that many aspects of internal auditing, under electronic operations, are exposed to various threats. The problem lies in the fact that IAs may struggle to track financial processes and transactions due to the absence of tangible financial records, which could affect the existing procedures and make it difficult to effectively and accurately assess the IA system.

In addition, lack of knowledge among IAs in programming, analysis, and design of electronic operating systems increases the risks associated with EAISs [20, 21]. Thus, the research problem can be summarized in the following two questions:

1. Do IAs in Libyan oil companies have the necessary competence and capabilities when auditing EAISs?
2. Do IAs in Libyan oil companies implement sufficient safeguards to address the risks associated with EAISs?

Given these research questions, two objectives are established, the first being to assess the competence and capability of IAs in the security of EAISs, and the second to determine the extent to which IAs implement adequate safeguards to mitigate the risks associated with EAISs. From the above review of the literature two research hypotheses are therefore formulated as follows:

1. Internal Auditors possess a high level of competence and efficiency in electronic accounting information system security.
2. Internal Auditors follow all protective measures to counter the risks of electronic accounting information systems.

### 3. Research Methodology

The study employed a descriptive-analytical approach, combining both secondary and primary sources for data collection. The secondary sources comprised the review of the accounting literature related to the study topic, and these provided the theoretical basis for the study. The primary data was gathered from a questionnaire specifically designed for the purpose. This data is of the first quarter of year 2023.

#### 3.1. Study Population

The study population consisted of employees from the Finance Departments and Internal Audit Departments in the Libyan NOC Joint Venture companies operating in Tripoli. A survey method was used, meaning that questionnaires were distributed to all targeted individuals. To increase the response rate, questionnaires were delivered directly to participants with instructions not to discuss the questions or answers with colleagues. Of the 45 questionnaires distributed (15 per company), 32 were returned, and 4 were deemed unusable for analysis. Therefore, 28 questionnaires were used for statistical analysis. Table 1 presents the number of questionnaires distributed, returned, and usable for statistical analysis.

#### 3.2. Questionnaire Design and Validation

**Questionnaire Development:** An instrument using closed questions was devised to collect data, with a focus in three areas as follows: Section 1 gathered demographic data and included five items. Section 2 focused on determining the IA’s competence in assessing the security of EAISs and included ten items. Section 3 addressed the extent to which the IA implemented sufficient protective measures to address the risks of EAISs and included nine items.

A five-point Likert scale was used to measure participants’ agreement/disagreement, scoring 5 for ‘Strongly Agree’, 4 for ‘Agree’, 3 for ‘Neutral’, 2 for ‘Disagree’ and 1 or ‘Strongly Disagree’. This scale tested feelings around the research statements and was used to determine the length of the scale used in the study’s axes (lower and upper limits). The range was calculated by subtracting the minimum value from the maximum value and then divided by the number of scale intervals (five) to obtain the interval length. The interval length was then added to the minimum value (1) to determine the upper limit of the first interval<sup>3</sup>.

To ensure the reliability of the questionnaire, both internal consistency and the reliability coefficient were tested. Internal consistency refers to the strength of the

relationship between each statement in a section and the total score for that section. Tables 2 and 3 present the results of the internal consistency, showing the correlation coefficients at the .01 and .05 significance levels. The results indicate a correlation between the statements of each section and the total score for that section.

Table 2 shows the correlation coefficients between the statements in Section 2 of the questionnaire, which measures the IA’s capacity and competence in assessing the security of EAISs and gives the total score of the section. All statements except one are seen to be significantly correlated with the total score at the .01 level, while the remaining statement is significantly correlated at the .05 level. This indicates a high degree of internal consistency among these statements.

Table 3 displays the correlation coefficients between the statements in Section 3 of the questionnaire which is related to the extent to which IAs implement safeguards to address risks facing EAISs and provides the total score for the whole section. It is evident that all statements are correlated with the total score at a significance level of .01, except for one statement that is correlated with the total score at a significance level of .05. This indicates internal consistency among the statements. In addition, the Cronbach’s alpha coefficient is used to determine the degree of reliability and consistency of the statements in each hypothesis proposed by the study. Table 4 presents the results of this test.

As indicated in Table 4, the alpha values exceed the accepted statistical value in the humanities, which is .600. This suggests that the questionnaire is reliable.

**Table 1.** Questionnaire Distribution, Return and Usability for Statistical Analysis

Company Name	Distributed	Returned	Unusable	Usable
Mabruk Oil Operation Company	15	11	1	10
Mellita Oil & Gas Company	15	10	2	8
Harouge Oil Operation Company	15	11	1	10
<b>Total</b>	<b>45</b>	<b>32</b>	<b>4</b>	<b>28</b>

<sup>3</sup> For more details about calculating the range and interval length see Appendix 2

The Role of Internal Auditors in Reducing Audit Risks  
Associated with Electronic Accounting Information Systems in Libya

**Table 2.** Correlation Coefficient Values between Statements in Section 2

No	Statements	Correlation Coefficient	Significance
1	The IA conducts their work relying on electronic systems (ES)	0.615**	0.000
2	The IA attends training courses on how to audit electronic systems (ES)	0.421*	0.026
3	The IA is capable of auditing EAISs with high efficiency	0.680**	0.000
4	The IA is concerned with assessing the risks associated with EAISs	0.764**	0.000
5	The IA monitors management's implementation of regular and periodic maintenance of (ES)	0.678**	0.000
6	The IA monitors employees' adherence to procedures that ensure the protection of EAISs	0.615**	0.000
7	The IA verifies that passwords are only used by authorized personnel	0.580**	0.001
8	The IA ensures that adequate security software is in place to scan electronic programs or magnetic disks	0.728**	0.000
9	The IA implements procedures to mitigate risks arising from electronic equipment damage	0.790**	0.000
10	The IA conducts periodic assessments of the Company's information security applications	0.589**	0.001

\*\* The correlation coefficient is statistically significant at significance of .01 level

\* The correlation coefficient is statistically significant at significance of .05 level.

**Table 3.** Correlation Coefficient Values between Statements in Section 3

No	Statements	Correlation Coefficient	Significance
1	The IA is informed of administrative decisions related to EAIS security procedures	0.718**	0.000
2	The IA is concerned with the implementation of electronic accounting information system security procedures	0.658**	0.026
3	The IA monitors information systems staff in carrying out required protection procedures	0.739**	0.000
4	The IA implements information security objectives such as privacy and timely data availability	0.685**	0.000
5	The IA participates in updating protection methods according to changes in the evolving IT environment	0.749**	0.000
6	The IA participates in developing security policies, such as selecting the appropriate technology and its effectiveness	0.785**	0.000
7	The IA participates in developing and designing a strategy for developing EAIS security	0.659**	0.001
8	The IA contributes to the discovery of security breaches through reports and descriptions of the type of breach	0.672**	0.000
9	There are alternative means of providing electronic services in the event of natural or man-made disasters	0.474*	0.000

\*\*The correlation coefficient is statistically significant at significance of .01 level

\*The correlation coefficient is statistically significant at significance of .05 level

**Table 4.** Results of Cronbach' Alpha Test

Section	No. of statements	Cronbach's alpha
The IA possesses a high level of competence and capability in assessing EAISs security	10	0.845
The IA implements a comprehensive set of safeguards to mitigate risks associated with EAISs	9	0.853

## 4. Data Analysis

In the tables which follow, Tables 5-9 present the Participants' Profiles. Table 10 reports descriptive statistics for the items assessing the capacity and competence of IAs in assessing risks related to EAISs, and Table 11 presents the descriptive statistics for the statements assessing the extent to which IAs follow comprehensive protection procedures to counter the risks of EAISs. Tables 12 and 13 then indicate the results of the hypothesis testing.

Table 5 presents an analysis of the data related to the participants' job titles from which it is seen that 60.7% of the respondents are Internal Auditors, 25% are accountants, and 14.3% hold supervisory positions (managers or heads of department).

**Table 5.** Participants' Job Titles

Description	Numbers	Percentage
Directorate Manager	3	10.70%
Head of Department	1	3.60%
Internal Auditor	17	60.70%
Accountant	7	25.00%
Total	28	100%

Table 6 presents details of the participants' educational qualifications, showing that 17.8% of respondents do not hold a university degree in their field of specialization, 71.5% hold university degrees, and 10.7% hold advanced degrees in their field of specialization.

**Table 6.** Participants' Educational Qualifications

Description	Numbers	Percentage
Undergraduate	2	7.10%
Higher Diploma	3	10.70%
BSc	20	71.50%
MSc	3	10.70%
PhD	0	0%
Total	28	100%

Table 7 indicates the participants' field of study, revealing that 85.7% of them hold a qualification in accounting and the rest are in some aspects of finance, economics or management.

**Table 7.** Participants' Field of Study

Description	Numbers	Percentage
Accounting	24	85.70%
Management	2	7.10%
Banking and Finance	1	3.60%
Economy	1	3.60%
Total	28	100%

Table 8 reports the participants' years of experience, reporting that the vast majority of respondents (71.4%) have ten or more years of experience, 25% have between five and ten, while only a small minority of 3.6% have less than five years of experience.

**Table 8.** Participants' Years of Experience

Description	Numbers	Percentage
less than 5 years	1	3.60%
5 years to 10 years	7	25.00%
More than 10 years	20	71.40%
Total	28	100%

Table 9 presents an analysis of the data related to the accounting system implemented in the companies studied. It shows that the accounting system in use in the three companies is a hybrid, involving the use of both manual and electronic systems.

**Table 9.** Company Accounting System

Description	Numbers	Percentage
Manual Accounting System	0	0%
Electronic Accounting System (EAS)	0	0%
Manual and EAS	28	100%
Total	28	100%

### 4.1. Evaluation of Internal Auditors' Competence and Efficiency in Electronic Accounting Information Systems

Table 10 presents the descriptive statistics for the items assessing the capacity and competence of IAs in assessing risks related to EAISs. Here it is seen that the mean scores for these items range from 3.39 to 4.21. The highest mean was for statement number 2, indicating that IAs had attended training courses on EAISs; conversely, the lowest mean was for statement number 10, suggesting that IAs did not consistently evaluate their companies' information security applications.

**Table 10.** Evaluation of Internal Auditors' Competence and Efficiency in Electronic Accounting Information Systems

	Statement	Mean	Std Dev.	Upper Value	Lower Value	Result
1	The IA conducts their work relying on electronic systems.	4.04	0.881	5	2	Agree
2	The IA attends training courses on how to audit electronic systems.	4.21	0.787	5	2	S.Agree
3	The IA is able to audit EAISs efficiently	4.00	0.861	5	2	Agree
4	The IA is concerned with mitigating the risks of EAISs	3.79	0.833	5	2	Agree
5	The IA monitors the management's implementation of regular and periodic maintenance of electronic systems	3.50	0.839	5	2	Agree
6	The IA monitors the employees' adherence to procedures that ensure the protection of EAISs	4.11	0.629	5	3	Agree
7	The IA ensures that passwords are only used by authorized personnel.	4.14	0.803	5	3	Agree
8	The IA ensures the existence of sufficient protection programs to scan electronic programs or magnetic disks.	3.64	0.870	5	2	Agree
9	The IA implements procedures to mitigate risks arising from damage to electronic equipment.	3.57	0.920	5	2	Agree
10	The IA conducts periodic assessments of the company's information security application	3.39	0.956	5	1	Neutral
	<b>Average descriptive statistic for statements related to the evaluation of the IA's competence and efficiency in assessing the security of EAISs</b>	<b>3.84</b>	<b>0.544</b>			<b>Agree</b>

**Table 11.** Evaluation of the Extent to which Internal Auditors Follow Comprehensive Protection Procedures to Counter the Risks of Electronic Accounting Information Systems

	Statement	Mean	Std Dev.	Upper Value	Lower Value	Result
1	The IA is aware of the administrative decisions related to EAIS security measures	3.71	0.659	5	2	Agree
2	The IA is interested in implementing security measures for EAISs	3.93	0.604	5	2	Agree
3	The IA monitors information systems staff in the implementation of required protection measures.	3.57	0.920	5	2	Agree
4	The IA implements information security protection objectives such as privacy and timely data availability.	3.71	0.713	5	2	Agree
5	The IA participates in updating protection methods according to changes in the evolving IT technology environment.	3.46	0.838	5	1	Agree
6	The IA participates in developing specific security policies such as selecting the appropriate technology and its effectiveness.	3.61	0.916	5	2	Agree
7	The IA participates in developing and outlining a strategy for developing the security of EAISs	3.61	0.832	5	2	Agree
8	The IA contributes to the discovery of hacking incidents via reports and describing the type of hack.	3.39	0.994	5	2	Neutral
9	There are alternative means of providing electronic service in the event of natural or unnatural disasters.	3.68	0.772	5	2	Agree
	<b>Average of the descriptive statistics for the statements related to evaluating the extent to which the IA follows comprehensive protection procedures to counter the risks of EAISs</b>	<b>3.63</b>	<b>0.552</b>	<b>5</b>	<b>2</b>	<b>Agree</b>

A review of Table 10 reveals a slight discrepancy among participants regarding their responses to the items related to this hypothesis. The mean score for responses to eight items falls within the ‘agree’ range, one item within the ‘strongly agree’ range, and one within the ‘neutral’ range. The overall mean score for all items (Agree)<sup>4</sup> was 3.84. Thus, the argument that IAs possess the competence and efficiency in assessing the security of EAISs is upheld.

**4.2. Evaluation of the Extent to which Internal Auditors Follow Comprehensive Protection Procedures to Counter the Risks of Electronic Accounting Information Systems**

Table 11 presents the descriptive statistics for the statements assessing the extent to which IAs follow comprehensive protection procedures to counter the risks of EAISs. These show that the mean scores for the items fall within the range of 3.39 - 3.93. The highest mean was for item number 2, which indicates the IAs’ interest in applying EAIS security measures. The lowest weighted mean was for statement number 8, which refers to the IAs’ contribution to the task of discovering hacking incidents through reports and describing the type of hack.

In Table 11, a slight discrepancy can be observed among participants’ responses to the statements related to this hypothesis. The mean score for most items falls within the ‘agree’ range, while one item falls within the ‘neutral’ range. The overall mean score (Agree)<sup>5</sup> for all items is 3.63, suggesting that the IAs do follow comprehensive protection procedures to counter the risks facing EAISs.

**4.3. Hypothesis Testing**

To test the research hypotheses, a one-sample t-test was used at a significance level of 0.05. The first hypothesis tested was:

H1 IAs possess a high level of competence and efficiency in EAIS security.

Table 12 presents the results of the one-sample t-test for H1, the first research hypothesis. Comparing the calculated t-value to the critical t-value of 2.042, we observe that the calculated t-value is greater than the critical t-value, and the significance level is less than 0.05. Therefore, we accept the first research hypothesis and conclude from the participants’ responses that IAs in the three studied companies have a high level of competence and efficiency in assessing the EAIS security.

**Table 12.** One Sample t-test Results for H1

Hypothesis	t - Value	Significance
IAs possess a high level of competence and efficiency in EAIS security	4.177	0.000

<sup>4</sup> For more explanation see Appendix 2

<sup>5</sup> For more explanation see Appendix 2

The second hypothesis tested was: H2 IAs follow all protective measures to counter the risks of EAISs.

Table 13 presents the outcomes of the one-sample t-test for H2. Comparison of the calculated t-value in the table with the critical t-value of 2.042, reveals that the calculated t-value is larger. Furthermore, the significance level is less than 0.05. Consequently, the second research hypothesis is upheld, and it is confirmed that the respondents from the studied companies follow all protective measures to counter the risks of EAISs.

**Table 13.** One Sample t-test Results for H2

Hypothesis	t - Value	Significance
IAs follow all protective measures to counter the risks of EAIS	2.119	0.043

**4.4. Results**

The results show that: IAs in the studied companies possess a high level of competence and efficiency in EAIS security and that they also follow all protective measures to counter the risks associated with EAISs. However, the analysis of the descriptive statistics shows that the mean scores of participants’ responses regarding the competence and efficiency of internal auditors in EAISs security were lower than the overall mean of the axis and this could be seen as a deficiency on the part of IAs in the following areas:

Reviewing risks related to electronic accounting information systems, monitoring management’s implementation of regular maintenance of electronic systems, ensuring the existence of sufficient protection programs to scan electronic programs or magnetic disks, implementing procedures to limit risks arising from electronic equipment damage, and periodically evaluating information security applications within the company.

The analysis of the descriptive statistics also reveals that the average scores of participants’ responses regarding IAs’ adherence to all protective measures to counter the risks of EAISs were lower than the overall mean of the axis, and again, this could be seen as a deficiency on the part of IAs but in this case, in the following areas:

Monitoring IT staff in implementing required security measures, participating in updating security methods according to changes in the evolving IT environment, participating in developing specific security policies such as selecting the appropriate technology and its effectiveness, participating in developing and formulating a strategy for developing the security of EAISs, and contributing to the detection of security breaches through reports and describing the type of breach.

## 5. Findings and Discussion

The Evaluation of Internal Auditors' Competence and Efficiency in Electronic Accounting Information Systems is presented in Table 10, and the Evaluation of the Extent to which Internal Auditors Follow Comprehensive Protection Procedures to Counter the Risks of Electronic Accounting Information Systems is presented in Table 11. Further, both research hypotheses H1 and H2 are supported as shown in Tables 12 and 13.

However, it is observed that, for instance, the statement number 5 in Table 10 *The IA monitors the management's implementation of regular and periodic maintenance of electronic systems* scores a mean of 3.50 which is lower than the average descriptive statistics for statements related to the evaluation of the IA's capability and efficiency in EAISs security with a mean score of 3.84. This might be the result of weakness on the part of IAs in monitoring the management's implementation of regular and periodic maintenance of EAISs. In addition, it is noted that, for example, the statement number 5 in Table 11 *The IA participates in updating protection methods according to changes in the evolving IT environment* scores a mean of 3.46 which is lower than the average of the descriptive statistics related to evaluating the extent to which the IA follows comprehensive protection procedures to counter the risks of EAISs with a mean score of 3.63.

In the context of previous research, our findings are in line with the results of those referenced [9, 12, 14, 15, 17, 18, 20]. One might argue that the development and advancement in IT enforce the shift and convergence from the manual accounting system to the electronic one. Here it must be noted that while the results obtained in previous studies are in the context of different environments where accounting systems might have different characteristics, our results are nonetheless similar to and consistent with them.

## 6. Conclusions and Recommendations

In conclusion it can be understood that there are certain weaknesses in the IAs' ability to effectively monitor management's commitment to the shift from manual to EAISs, and that this poses an ongoing threat to the security of accounting information in the scenario where the current hybrid systems seen to operate in the companies examined give way incrementally to the introduction of EAISs that are not supported by manual processes which is currently the case. Therefore, four strong recommendations are made as follows:

- Encouragement to company management to provide adequate support to both the IA department and its employees to ensure the maintenance and development of IAs' competence and efficiency in EAISs security.

- Encouragement to the IA department and its employees to consistently follow all protective measures to counter the risks of EAISs systems and to continuously improve these measures.
- Encouragement to the IA department to focus more on developing the competence and efficiency of its IAs. This might be done through the following procedures: reviewing risks associated with EAISs, monitoring management's implementation of regular and routine maintenance of electronic systems, ensuring the existence of sufficient protection programs to scan electronic programs or magnetic disks, implementing procedures to limit risks arising from electronic equipment damage, and periodically evaluating the company's information security applications.
- Encouragement to the IA department to pay more attention to reviewing and evaluating the adequacy and effectiveness of all procedures and methods related to addressing EAISs risks included in the Internal Audit Plan in the following areas: monitoring IT staff to ensure they are implementing required security measures, participating in updating security methods according to changes in the evolving IT environment, participating in developing specific security policies such as selecting the appropriate technology and its effectiveness, participating in developing and formulating a strategy for developing the security of EAISs and contributing to the detection of security breaches through reports and describing the type of breach.

One limitation to this research is that this study does not include participants from other sectors such as banking or from other public firms. Conducting further research, on the role of IA in addressing specific EAISs risks is therefore essential, and could focus for example, on: identifying the extent to which IA departments and their staff have the necessary capabilities to address these risks, assessing the role of IA departments and their staff in mitigating these risks, and evaluating the integration of roles between internal and external auditors in addressing the risks. Future research may incorporate participants from other sectors experiencing a shift from manual IA of accounting systems to electronic accounting systems IA. Our study findings will provide important insights for regulators and policymakers at top managerial levels in respect of companies' strategic planning processes in an era of vibrant business environment and advancement in IT systems, one being the auditing of EAISs.

## Appendixes

**Appendix 1:** The National Oil Corporation (NOC) was established on 12 November 1970, under Law No: 24/1970, replacing the general Libyan Petroleum Corporation which

established under Law No. 13 of 1968 to assume the responsibility of the oil sector operations. It was later reorganized under decision No: 10/1979 by the General Secretariat of the General People's Congress, to undertake the realization of the objectives of the development plan in the areas of petroleum, supporting the national economy through increasing, developing and exploiting the oil reserves and operating and investing in those reserves, to realize optimum returns. In carrying out its activities, the NOC may enter into participation agreements with other companies and corporations carrying out similar activities.

**Appendix 2:** A five-point Likert scale was used to measure participants' agreement with each item, with 'Strongly Agree' scored as 5, 'Agree' as 4, 'Neutral' as 3, 'Disagree' as 2, and 'Strongly Disagree' as 1. The study relied on this scale to test the statements and to determine the length of the scale used in the study's axes (lower and upper limits). The range was calculated, which was divided by the number of scale periods (five) to obtain the period length. After that, the period length value was added to the lowest value on the scale, being one, to determine the upper limit of the first period and so on for the rest of the periods as follows:

Range: The highest value on the scale - the lowest value on the scale (5-1 = 4) Period length =  $4/5 = 0.80$ . The upper limit of the period = the lower limit + period length. Thus, the upper limit of the first period =  $1 + 0.80 = 1.80$  and so on for the rest of the periods.

The following criterion was used to judge the opinion of the study sample:

- If the value of the arithmetic mean is from (1) to (1.80), the degree is (strongly disagree).
- If the value of the arithmetic mean is from (1.81) to (2.60), the degree is (disagree).
- If the value of the arithmetic mean is from (2.61) to (3.40), the degree is (neutral).
- If the value of the arithmetic mean is from (3.41) to (4.20), the degree is (agree).
- If the value of the arithmetic mean is from (4.21) to (5.00), the degree is (strongly agree).

Example: If the mean score for a particular question (statement) was 3.2, it would be categorized as 'neutral' because it falls between 2.61 and 3.40.

## REFERENCES

- [1] Alzoubi, E. S. S, "Audit committee, internal audit function and earnings management: Evidence from Jordan," *Meditari Accountancy Research*, Vol. 27, No. 1, pp. 72-90, 2019. URL: <https://doi.org/10.1108/MEDAR-06-2017-0160>
- [2] AL-Mashhadi, A.S.J, "Review on Development of the Internal Control System," *Journal of Accounting Research, Business and Finance Management*, Vol. 2, No. 1, pp. 12-20, 2021. URL: <file:///C:/Users/DELL7/Downloads/Re>
- [3] Pickard, M. D., Schuetzler, Valacich, J. S., & Wood, D. A. "Innovative accounting interviewing: A comparison of real and virtual accounting interviewers". *The Accounting Review*, Vol. 95, No. 6, pp. 339-366, 2020. URL: <https://doi.org/10.2308/tar-2017-0235>
- [4] National Oil Corporation (NOC). "To enhance transparency and reinforce the oversight role of internal audit departments", the Chairman of the Board held a meeting with directors of internal audit departments and offices in oil companies". <https://noc.ly/%D8%AA%D8%B9%D8%B2%D9%8A%D8%B2-%D9%85%D8%A8%D8%AF%D8%A3-%D8%A7%D9%84%D8%B4%D9%81%D8%A7%D9%81%D9%8A%D8%A9-%D9%88%D8%A7%D9%84%D8%AA%D8%A3%D9%83%D9%8A%D8%AF-%D8%B9%D9%84%D9%89-%D8%A7%D9%84%D8%AF%D9%88> (accessed September. 23, 2024).
- [5] Al-Hamidi, N. A., Al-Ubaid, A. A. A., & Al-Samarai, S. A, "*Management Information Systems: A Contemporary Approach*", 1<sup>st</sup> edition, Dar Wael for Publishing. Amman, Jordan, 2004.
- [6] Al-Eisi, Y.A, "*Fundamentals of Modern Accounting*" *Part One*, Dar Alsharq for publication and distribution. Amman, Jordon, 2003.
- [7] Hassan A. H. A, "*Your Guide to Systems Analysis and Design*", Aldar-Aljameeya for publication and distribution. Cairo, Egypt, 2006.
- [8] Hashem, A, "Activating the Auditor's Role in Confronting the Risks of Electronic Accounting Information Systems Security," *Scientific Journal of Economic and Commerce*, Ain Shames University. Vol. 35, No. 1, pp. 155-206, 2005. URL: <https://search.mandumah.com/Record/111131>
- [9] Alqudah, H., Lutfi, A., Abualoush, S. H., Al Qudah, M. Z., AlshIR a'h, A. F. Almaiah, M. A., Alrawad, M., & Tork, M, "The impact of empowering internal auditors on the quality of electronic internal audits: A case of Jordanian listed services companies," *International Journal of Information Management Data Insights*, Vol. 3, No. 2, pp. 1-8, 2023. URL: <https://doi.org/10.1016/j.jjime.2023.100183>
- [10] El-Fyoumy, M, "EDP Auditing: A Review of Computerized Accounting Systems", Dar El-Ash'a for Publication. Alexandria, Egypt, 1993.
- [11] Al-Bahisi, E & and Al-Sharif, H, "Risks of Electronic Accounting Information Systems: An Applied Study on Banks Operating in the Gaza Strip," *Islamic University Journal*, Vol. 16, No. 2, pp. 895-923, 2008. URL: <file:///C:/Users/DELL7/Downloads/987-3180-1-PB.pdf>.
- [12] Al-Haithi, S and Al-Rabiahah, A.M, "The Impact of Security Threats on Information Security in Light of E-Governance Implementation: A Field Study in Several Jordanian Ministries and the Greater Amman Municipality," *Accounting, Management and Insurance Journal*, Vol. 44, No. 65, pp. 309-378, 2005. URL: <https://search.mandumah.com/Record/330124>
- [13] Daoud, H.T, "Information Network Security", King Fahd National Library, Reyad, Saudi Arabia, 2004.
- [14] Alsakni S. A, Al-Awadi, H, "Risks of Using Information Technology and Its Impact on the Performance of Accounting Information Systems - An Applied Study on a

- Sample of Joint Stock Companies Listed on the Amman Stock Exchange," *Information Studies Journal*, Vol, 14, pp. 207-257, 2012. URL: <https://search.mandumah.com/Record/206855>
- [15] Al-Saedi, S.O and Eqjam, K.A, "The Role of Internal Audit in Confronting Risks in Electronic Accounting Information Systems: A Case Study of Al-Zawiya Refining Company," *National Journal of Management*, Vol. 13, pp. 67-108, 2014. National Institute of Management, Tripoli, Libya.
- [16] Jamila, N, "The role of internal auditing in mitigating the risks of accounting information systems". Unpublished Msc thesis. Faculty of Economics, Commerce, Management, University of Ahmed Draia Adrar, Algeria, 2018. URL: <http://www.univ-adrar.dz/:8080/xmlui/handle/123456789/1134>
- [17] Mahmoud, O. A. A, "The role of internal audit in reducing the risks of electronic accounting information systems," *Journal of Economic, Administrative and Legal Sciences*, Vol. 1, No. 1, pp. 28-42, 2017. URL: <https://journals.ajsrp.com/index.php/jeals/article/view/168/135>
- [18] Omar, N. K, "The role of modern internal audit trends in mitigating accounting information security risks," *International Journal of Research and Studies Publishing*, Vol. 4, No. 39, pp. 530-552, 2023. URL: <https://www.ijrsp.com/pdf/issue-39/18.pdf>
- [19] Al-Shammari, A.D.J &Al-Grban, F.A.M, "The effect of using electronic auditing programs on auditing and oversight work," *Social Science and Humanities Journal*, Vol. 04, No. 06, pp. 1942-1953, 2020. URL: <file:///C:/Users/DELL7/Downloads/admin,+SSHJ+1.pdf>
- [20] Ekriem, H.M.M, "The Role of Internal Auditors in the Banking Sector in Mitigating Risks Associated with Electronic Accounting Information Systems: A Field Study," *Journal of Commercial and Environmental Studies*, Vol. 10, No. 1, pp. 150-189, 2019. URL: [https://jces.journals.ekb.eg/article\\_50373\\_d33e4d73dbddc121309f3904f894dc0a.pdf](https://jces.journals.ekb.eg/article_50373_d33e4d73dbddc121309f3904f894dc0a.pdf)
- [21] Saadi. I & Faraj, S, "The Role of Internal Audit in Mitigating the Risks of Electronic Accounting Information Systems: An Empirical Study on Libyan Oil Companies," *Journal of Accounting Studies*, Vol. 6, pp. 168-198, June 2024. The Libyan Accountants & Auditors Association publication. Tripoli, Libya.