Journal of Business and Environmental Sciences
Volume: 4(1), Page: 127-146
https://doi.org/10.21608/jcese.2024.321691.1079
ISSN: 2974-3117
E-ISSN: 2974-3125

Research article

The Role of Internal Audit in Enhancing Cyber Security From The Auditors' Point of View

Iman Babiker

Assistant Professor of Accounting College of Business Administration, Princess Nourah bint Abdulrahman University (PNU), (Riyadh), Saudi Arabia; iakhalid@pnu.edu.sa.

Abstract

Purpose: This study investigates the role of internal audit procedures in enhancing cybersecurity effectiveness. It seeks to answer key questions: Is the efficiency and effectiveness of internal audits indicative of proper cybersecurity standards? To what extent can audit committees improve internal audit efficiency and achieve information security? How do information security governance standards help mitigate cybersecurity risks? To address these questions, the opinions of 30 internal auditors from Saudi Arabia, Sudan, and Egypt were surveyed.

Methodology: A descriptive and analytical approach was used.

Findings: The findings reveal a positive relationship between the efficiency and effectiveness of internal audits and enhanced cybersecurity. Specifically, a more effective internal audit system correlates with stronger information security, and improvements in information security governance standards significantly reduce electronic risks.

Contribution and Value: This study emphasizes the crucial role of internal auditing in strengthening cybersecurity from the auditors' perspective, focusing on its impact on auditing frameworks and security strategies. As one of the few studies addressing this intersection, it provides valuable insights and recommendations for stakeholders in both fields. The research highlights the importance of internal auditing in protecting information confidentiality and mitigating risks, proposing innovative solutions aligned with technological advancements to enhance resilience against vulnerabilities. Ultimately, the study aims to foster discussions on effective risk management strategies in a rapidly evolving digital landscape.

Keywords: Internal audit, cybersecurity, information security risks.

APA Citation: Babiker I. (2025). The role of internal audit in enhancing cyber security from the auditors' point of view. *Journal of Business and Environmental Sciences*, 4(1), 127-146.

Received: 17 September 2024; **Revised**: 9 October 2024; **Accepted:** 13 October 2024; **Online:** 15 October 2024
The Scientific Association for Studies and Applied Research (SASAR)
https://jcese.journals.ekb.eg/

Introduction:

The impact of technological development in various aspects of life, and many business organizations have relied on information technology to conduct their business, because of its many benefits in facilitating tasks and shortening time and cost. As accounting is an important function for all business organizations, it is also concerned with keeping pace with technological development, and as long as the process of processing accounting information has become electronic, it must take into account the distinguished position occupied by that information and must keep abreast of developments and developments in the field of security and protection of information (Cyber Security).

Due to the important role of accounting information, it must always strive to find solutions that keep pace with the movement of technological progress and when keeping pace with this development and technology, it has achieved a sufficient amount of striving towards providing security and technology in order to reduce the chances of information exposure to potential risks and in the event of reaching a high level of security and protection policies for information, internal auditors can reach methods of detection and confrontation of potential risks.

Public and commercial businesses' increasing reliance on networks and information technologies for their financial management systems makes them more susceptible to cyber-attacks. Additionally, as the economy has grown increasingly knowledge-based, managers and accountants now place a high priority on safeguarding information assets. Thus, in a few of years, cyber security has grown to rank among the most important risk management issues facing all kinds of organizations. Ten years ago, for example, the IAF changed and adjusted to the growing significance of IT in all facets of company operations.(Haapamäki, E. and Sihvonen, J,2019).

Based on the above, it was not possible to maintain the professional practice of internal auditing in isolation from the developments of the end of the twentieth century and the beginning of the twenty-first century, whether of globalization, the tremendous economic and technical developments, the repercussions of the collapse of major global business companies, or the emergence of the concept of corporate governance, which is based on the internal audit profession as an important axis on which the success of companies is based.

The internal audit function has evolved and increased its importance as a result of the role it plays within the organization as an effective tool whose task is to examine and evaluate the efficiency and effectiveness of other control tools, and it is relied upon as an advisory function that improves risk management, and this development has gone through different stages, as environmental conditions and management needs contributed to its occurrence, and in determining the status of internal audit within the organization.

In our time, after the coronavirus pandemic and the great shift to relying on work through the Internet, holding meetings, and exchanging information and files remotely, the situation has become more urgent to maintain information security.

- The first axis: the methodological framework of literature review:

Study issue:

The study issue was formulated in the following questions:

1- Is the efficiency and effectiveness of internal audit evidence of the proper application of cyber security standards?

2- To what extent can audit committees play an active role in raising the efficiency of internal audits and achieving cyber security?

3- Do Information Security Government Standards Contribute to Reducing Cyber Risks Related to Information Security?

• Objectives of the study:

The study aims to know the extent to which internal audit contributes to achieving cyber security.

• Study hypotheses:

1- There is a statistically significant relationship between the efficiency and effectiveness of internal audits and the enhancement of cyber security.

2- There is a statistically significant relationship between the existence of audit committees as a tool of corporate governance and the achievement of cyber security.

3- There is a statistically significant relationship between improving information security governance standards and reducing cyber risks.

Research Gap:

After reviewing a wide range of research interested in cyber security, we found that there is a scarcity of research that is interested in highlighting the role of accounting and its branches in cyber security.

Limitations of the study:

The ability to draw broader comparative conclusions has been affected by the scarcity of studies linking information security and internal auditing. The researcher recommends that those interested in this field conduct studies that encompass wider communities. Additionally, it is suggested that future research in this area utilize personal interviews to gather opinions directly from respondents, allowing

for in-depth discussions and a more detailed understanding of their perspectives.

Structure of the study:

The study was divided into three axes:

1. Literature review.

2. the theoretical framework of the study.

3. Field study and result.

1. Literature Review:

This study aimed at several objectives, the most important of which are to Identify cyber security strategies and the role of modern technologies and challenges in reducing the risk of cyber-attacks, and know the role of modern technologies in securing cyberspace. And reveal the challenges facing him. And reached a set of results, the most important of which are Modern technologies contribute in protecting and securing information by monitoring and analyzing cyber-attacks As a result The imperative of modernizing and developing protection systems, identifying the most vulnerable points, and countering attacks (Al-Shawabkeh ،2019).

In the context of identifying the risks to digital information security in its various forms and countermeasures to reduce these risks, such as regulatory, physical and technical measures, in addition to legislative measures and the most important international standards set by the ISO organization to control information security practices, the study found that information security is exposed to many risks and threats that take place in the Internet environment with the difficulty of keeping pace with security countermeasures to the rapid development of modern methods used in attacks on information security. (Hassan ،2019).

Internal Audit plays an active advisory role in driving digital value by identifying risks and providing strategic advice.(Shehata, 2020).

(Al-Shehri 2020) pointed out that the challenges facing the protection of this space are the continuous development of malware, and to be confronted, national cadres must be trained and qualified, and effective software must be prepared that can address these risks.

This study focused on a problem that has become haunting the world, which is swimming in an endless space of cyberspace to live a virtual reality that is very complex and intertwined and surrounded by cyber risks from all sides, which drew the attention of researchers and research bodies in the developed world to develop control controls to ensure cyber security, in a way that provides protection against crimes and electronic violations that can cause serious damage at the level of countries, business

organizations or individuals, at the level of business organizations, the audit activity is concentrated Internal in evaluating and contributing to improving risk management, internal control and governance systems, through a systematic and risk-based approach aimed mainly at serving the department in achieving its objectives, hence, with the entry into the digital transformation environment, the internal audit activity extended to new burdens and responsibilities as it represents one of the most important lines of defense for the organization. (Attia ،2021).

The recent occurrence of this digital transformation and the tendency of most businesses after the coronavirus pandemic to deal online this change has increased and transformed Cyber Attack Risks Moreover, due to this digitization, it has become difficult to manage fraud risks, as traditional internal controls are ineffective to counter this transformation. (Abdelmoneim Bahyeldin ،2022).

Stakeholders, especially investors, will not be able to follow up on cyber risk operations without the help of an internal audit, since based on the capabilities provided by the internal auditor in a rational manner, it will achieve the maximum return and benefit that corresponds to the requests and needs of investors. as (Jihan Adel ،2022).

The extent of cyber security audits by Internal Auditor Highly and positively correlated efficiently with Internal Auditor in relation to governance, risk, and control. (Md. Shariful Islam ،2018).

Commenting on previous studies:

The objectives of previous studies varied and differed in dealing with the subject of cyber security and internal audit with different methodologies, some studies dealt with the role of information security and protection from the point of view of internal auditors and others focused on the risks to digital information systems.

2. Theoretical Framework

Cyber Security:

This field of technology, also known as "computer security" and "information security," is concerned with defending systems, assets, networks, and programs against online threats that typically try to obtain, alter, or destroy private data, demand ransom from users, or interfere with commercial operations. Work information systems, improve data security, privacy, and confidentiality, and take all required precautions to shield customers and citizens from online dangers.

Governments and individuals can use cyber security as a strategic weapon, particularly as cyber warfare is now a fundamental component of contemporary attack and warfare strategies. ((Al-Sawalhi ،2024).

Information in our time and present time has become rapidly spreading, and this has contributed to the

technological development in the field of communications, and this information has become easy to circulate through Internet services, this matter has led to the emergence of many risks and attacks that take place in this environment (Internet environment), which calls for the need to secure and protect this information. (Gharbi ،2022).

Cyber security has become a fundamental aspect of national security policies globally, reflecting the concerns of various stakeholders, including utilities, regulators, energy markets, and government agencies. As cyber warfare increasingly serves as a method of conflict and a strategic tool for military planners, it can also be exploited by governments for their own interests. Meanwhile, cybercriminals have access to a wide range of new tools and technologies, enabling malicious activities to occur virtually anywhere. This chapter examines the emerging laws, policies, processes, and tools that are reshaping the cyber security landscape. (Dwson, 2015).

Many countries have developed legislation that protects information security and there are a number of organizations that develop international standards that are considered an optimal guide used to protect information.(Taha,2020).

Cyber security has a wide-ranging impact on facilities, making some organizations vulnerable to hacker and ransom ware attacks. With the advancement of technology and the push of the pandemic COVID-19 As companies adopt remote working arrangements, companies are dealing with new and evolving cyber security threats. In response, regulators, investors, stakeholders, and ordinary people want to learn more about the cyber security risks facing businesses and organizations. (Mahmoud ، 2022).

Cyber security threats are a growing global problem. Countries, including the Gulf states in particular and the Middle East in general, face a range of complex threats as they seek to exploit their digital economies, in addition to attacks against systems that manage critical national infrastructures, (CNN in Arabic, 2021).

The risks facing countries will increase due to the repercussions and effects of the Corona pandemic, the increasing reliance on remote communication at work, distance learning, and the increasing amount of data that is relied upon. The World Economic Forum's Cyber security Center predicts that 74% of companies will be hacked in 2022. (CNN, 2021).

Cybercrime represents the most serious type of crime committed through the Internet, and this is illustrated by looking at the gravity of the losses that can be caused by a single successful operation that falls under its concept. (Muslim,2021).

If we reflect on the current reality and the data available around us, we find that the implementation of effective cyber security measures represents a major challenge today due to the abundance of hardware

and software and the dependence of most companies and institutions in all industries on computers, software, and accessories, including networks and others.

What is the goal of cyber security?

The main goals of information protection are to ensure the confidentiality, integrity and availability of information. Any event or issue that threatens the security triangle (confidentiality, integrity and availability of information) represents a security threat that must be addressed and resolved, or mechanisms or procedures must be implemented to avoid it or minimize its impact.

Security should be integrated into software and operating systems to ensure the required level of protection, as companies now face increasing risks, such as cyberattacks. (Lois et al., 2021).

Information security has become important because it affects organizations in almost all fields and industries, and data breaches affect millions of customers and cost organizations millions of dollars (Thiagarajan Ramakrishnan ،2022).

We do not need to talk about the importance of information security because it has become a given in this era, and information security is considered Very strategically important, and senior management has a pivotal role to play in establishing and managing information security in the company. (Solms ، 2001).

Internal audit and its relationship to information security protection:

With attacks on critical infrastructure, businesses and countries on the rise, interest in cyber security has increased. (Yuchong Li a b, 2021).

Accounting parameters have an important role in helping decision makers of all kinds, whether internal or external, and it has become necessary for traditional accounting to find its way to keep pace with technological development to the extent that provides security for accounting information from potential risks. Here, the role of internal audit is highlighted in developing methods that enable the detection of types of risks and mechanisms. Detect and avoid them.

The internal audit function has evolved and increased its importance as a result of the role it plays within the organization as an effective tool whose task is to examine and evaluate the efficiency and effectiveness of other control tools, and it is relied upon as an advisory function that improves risk management, and this development has gone through different stages, as environmental conditions and management needs contributed to its occurrence, and in determining the status of internal audit within the organization. (Suleiman ،2006).

Managers should recognize Internal Audit as a crucial element in mitigating Cyber Security risks and enhancing proactive measures. (Elmaasrawy & Tawfik, 2024).

Cyber risk is not something that can be avoided; rather, it must be managed. Hence, it is very important to maintain official documents related to relevant cyber controls. Internal audit should be an integral part of the cyber security assurance process, as internal audit is uniquely positioned to look across organizations. The contribution of internal audit also provides comfort to the Board and the Audit Committee. (Sezer Bozkus Kahyaoglu, 2018).

A researcher observed a strong correlation between investment structure and the perceived advantages of the cyber security risk framework for investors. The perceived benefits of the risk framework and investment intent are also positively impacted by high-quality information and understanding of cyber security. (Ling Yang ،2020).

Stakeholders, especially investors, will not be able to follow up on cyber risk operations without the help of an internal audit, since based on the capabilities provided by the internal auditor in a rational manner, it will achieve the maximum return and benefit that corresponds to the requests and needs of investors. (Jihan Adel ،2022).

The extent of cyber security audits by Internal auditors highly and positively correlated efficiently with Internal auditors in relation to governance, risk, and control. (Md. Shariful Islam ،2018).

The role of internal audit in risk management:

Risks are one of the most important challenges faced by economic units and work to avoid their occurrence in the future and are defined as future events expected to occur that negatively affect the results of the economic unit, its objectives, plans and strategies, and risks cover all operations and arise as a result of the absence of internal factors related to the nature of the facility and the efficiency of workers and other external factors related to economic and technological conditions and new legislation. (Abdel Aal ،2006) The internal auditor's cooperation with the information technology team provides more efficient and reliable information. (Kurniawan & Mulyawan, 2023).

Cyber security risk management means that companies adopt an appropriate methodology that enables them to implement and operate control controls that help protect their information systems and assets and improve the process of managing these risks Companies need to develop awareness and interest in ensuring good practices in the field of security risk management Seeb Rani and adopt a more flexible methodology to respond to new and evolving cyber threats in order to maximize the benefits to the company from effective cyber security risk management. (Ali and Ali, 2022).

Risks are divided into types as follows: (Hammad ،2007).

Financial risks: These are related to investment, credit, and ability to repay obligations, and they include liquidity risk, credit, debt repayment, interest rate changes, foreign exchange rate, solvency risk, and capital adequacy risk.

Operational risks: They negatively affect the revenues and capital of the economic unit, and arise as a result of making wrong decisions that do not keep pace with modern changes and include information risks, modern technical and technological risks, fraud, and incompatibility in the implementation of administrative policies and procedures.

Strategic risks: It is related to changes in the competitive environment, the industry that operates in the field of economic unit, and changes in the sectors of preparing customer orders, and they include risks beyond the control of the enterprise, such as laws, regulations, and political and economic restrictions.

Moral risk: It includes the risks that arise from the asymmetry of information between internal parties and external investors, and this type appears in the event of a conflict of interest between multiple parties.

The responsibilities that must be included in the internal audit tasks in the field of risk management are:
Give assurance on the effectiveness of risk management processes.
Risks are properly assessed.
Assess the reporting of key risks, follow up and review the key risk management process and assist in the identification and assessment of risks.
Train management and assist it in risk response procedures.
Provide proposals related to the risk management strategy to the Board of Directors for decision.
Types of security risks
Security risks can be classified into: (Al-Shawabkeh ،2019).
Natural hazards: Natural hazards such as storms that can create a massive power surge can reduce the effectiveness or performance of networks and computers.
Intentional human hazards: such as deliberate intrusions or cyber-attacks.

Malicious acts can also be committed against the organization's network resources by persons operating inside and outside the network. Without proper security controls, a hacker will be able to infiltrate the facility's network, steal data, or affect the network's ability to provide services, and internal employees if ignored may commit espionage against the company. Unintentional human hazards: such as accidental cancellation, typing errors, lack of awareness and training, or errors in unintentional entry.

Security risks

Information security risks can negatively impact an organization, its operations, assets and employees, and can pose a threat to other organizations. Moreover, the occurrence of these risks can lead to a decrease in the market value of an organization, as it threatens the confidentiality, integrity and availability of accounting information processed, stored, sent or disclosed by electronic accounting

information systems. Therefore, many organizations resort to the application of information security governance, which aims to protect electronic assets from a variety of potential risks by using a set of widely used international standards to ensure that the necessary and adequate level of security is achieved.

Cyber security is one of the most important issues that management and boards of directors have paid attention to, and it is very important in all companies, and it is important to have AICPA The goal of establishing a common basic language for cyber security risk management reporting. (Sihvonen, 2019)

3. Field study:

3.1 Introductions:

This section includes a description of the study population and sample, the statistical techniques used to analyze the data and test the study hypotheses, and the field study procedures, which include how to collect data, process it statistically, interpret it, and run reliability and validity tests to ensure its validity.

3.2 Study Methodology:

Due to the nature of the research and the information to be obtained, the study relied on the descriptive analytical approach, which relies on studying the phenomenon as it exists in reality and is concerned with describing it as an "accurate" description and expressing it in "qualitative" and quantitative terms. The qualitative expression describes the phenomenon to us and explains its characteristics, while the quantitative expression gives us a description. "Digitally" shows the extent or magnitude of this phenomenon and the degrees of its connection with other phenomena. In addition, the use of the descriptive analytical method is compatible with the nature of the problem that is the subject of the study, which sheds light on its various aspects through narration and focused.

3.3 Study Population and sample:

Based on the problem of the study and its objectives, the target population consists of auditors and accountants in addition to specialized academics. The research items were selected from the study population described in the previous paragraph through the purposive or intentional sampling method, which means selecting several cases or individuals on the basis that they achieve One or some of the purposes of the study that will be carried out. Naturally, these individuals must have an acceptable degree of objectivity in their statements and opinions and trust in them. Intentional, deliberate, or arbitrary selection, as some call it, is done through the intentional selection on the part of the researcher of a number of sampling units, where the researcher believes, according to his full knowledge of the study community, that they correctly represent the original community; This is in the event that it is limited to this sample. A number of (30) questionnaires were distributed electronically. The features of

the study sample are as follows:

It is clear from Table (1) below that the majority of the study sample members are internal auditors, with their percentage reaching (76.7%), while the percentage of the sample members are accountants (13.3%). We also find that the largest percentage of them have more than ten years of experience, as their percentage reached (50%)

Table 1: Features of the research sample participants

Sample characteristics	Categories	frequency	percentage
1/Profession	internal Auditor	23	76.7
	accountant	4	13.3
	General reviewer	1	3.3
	Specialized academic	2	6.7
2/ experience	One year	8	26.7
	From two to three years	3	10
	From four years to ten years	4	13.3
	More than ten years	15	50

Source: The researcher conduction from field study 2024

3.4 Study tool:

The study's major data collection method was obtaining the information required to determine internal audit's contribution to improving cyber security from the auditors' perspective. The standards created by experts served as the foundation for the preparation and development of the questionnaire. Consequently, there are two sections to the questionnaire: The study sample members' data are included in the first section. The study's fundamental concepts, which serve as the topics by which the study hypotheses are determined, are included in the second section.

The first axis: measures the hypothesis of the first study (There is a statistically significant relationship between the efficiency and effectiveness of internal auditing and enhancing cyber security) and includes several (7) statements.

The second axis: measures the hypothesis of the second study: (There is a statistically significant relationship between improving information security governance standards and reducing electronic risks) and includes several (7) statements.

3 .5 Data Measurement:

For the purpose of measurement, the researcher used Likert Scale Pentathlon to gauge the likely range of replies. The weight distribution for the respondents' answers is as follows: the highest weight, which is assigned five degrees, indicates "strongly agree," while the lowest weight, assigned one degree, indicates "strongly disagree," falling between the other two weights. That is done so that respondents may select the precise response at their own choice. The degree to approve measure is shown in Table (2).

Table (2) determines the degree of measure approval.

Approved Degree	Relative weight	%	Statistical Significance
Strongly Agree	5	Greater than 80%	Very high degree of Approval
Agree	4	70 – 80%	high degree of Approval
Neutral	3	50 – 69%	Medium
Disagree	2	20 – 49%	Low approval
Strongly disagree	1	Less than 20%	Very Low approval

Source: The researcher conduction from field study 2024

3.6 Reliability and Validity:

To measure the validity of the study tool, the study relied on:

a- Content validity:

To verify the validity of the scale, the study relied on apparent validity, as it was presented The draft measurement tool was presented to a group of arbitrators and specialized experts in the subject area of the study.

b- Internal consistency validity:

The correlation coefficient values were estimated for all axes with the total score, and the following is a table showing the test results:

Table No. (3) Correlation coefficient of the study axes with the total

Field	Correlation coefficient	P-value(sig)
First hypothesis	0.86	0.0000
Second hypothesis	0.81	0.0000

Source: The researcher conduction from field study 2024

It is clear from Table (3) that all the study's axes have a positive and statistically significant correlation

at the significance level (0.05) with the total sum of the axis to which they belong. Thus, all dimensions of the tool are considered to measure what they were designed to measure.

3.7 Reliability of the Research:

This study used Cranach's Alpha Coefficient to test the reliability of each of its instrument's dimensions and subscales.

Table (4) presents a summary of the reliability analysis results. Verified that every scale exhibits a reasonable degree of reliability (Cranach's alpha is greater than the cutoff point of 0.6). As a result, it may be said that the reliability of the measurements is adequate.

Table No. (4) Results of Cronbach's alpha test for the study's axes scale

Dimension	Number of Items	Coefficient
First hypothesis	**7**	**0.84**
Second hypothesis	**7**	**0.80**
All items	**14**	**0.86**

Source: Prepared by the researcher from field study data 2024

3.8 Test for normal distribution of data:

This test is thought to be essential for selecting the proper test for the significance of the differences since it seeks to determine whether or not the data has a normal distribution. The Kolmograv-Smirov test was employed to guarantee that the data is distributed in a way consistent with a normal distribution: The normal distribution test findings for the study hypotheses' axes are as follows.

Table No. (5): Results of the normal distribution test for the study variables.

Dimension	Z-value	P-value(sig)
First hypothesis	**0.432**	**0.84**
Second hypothesis	**0.486**	**0.80**

Source: The researcher conduction from field study 2024

From Table (5), it is clear that the value of the level significance for all axes of the study hypotheses is less than (0.05). These values mean that the data for all axes of the study are not characterized by a normal distribution, which indicates the possibility of using non-parametric tests (chi-square test) to test the significance of the differences, as It indicates that the results that the study will reach through the use of these tests accurately reflect the population from which the sample was taken.

3.9 Statistical Treatment:

To analyze the data and test the hypotheses, a variety of statistical tools were utilized. The Statistical Package for the Social Sciences (SPSS) Version 26.0 was employed, applying the following techniques:

Conducting a reliability test for the questionnaire questions using "each of the following: a/ Apparent validity test. b/ Cronbach's Alpha coefficient." It was used to measure the internal consistency of the study statements to verify the validity of performance. Arithmetic mean: This statistical method was adopted to describe the sample members' opinions about the study's axes.Standard deviation: This measure was used to determine the extent of dispersion in respondents' opinions about the study statements compared to the arithmetic mean. Chi-square test: This test is used to test the significance of differences at a significance level of 5%. This means that if the value of (chi-square) is at a significance level of less than 5%, the null hypothesis is rejected.

3. 10 Presentation an

d analysis of the study results:

In order to offer descriptive statistics (mean, standard deviation) for the fundamental data, the researcher intends to examine the data. The study hypotheses are then discussed in the following order, taking into account the relative importance of the study statements and the differences found using the chi-square test:

A. Presentation and analysis of the results related to the first hypothesis:

The first hypothesis states: (There is a statistically significant relationship between the efficiency and effectiveness of internal audits and enhancing cyber security).

To verify the validity of the hypothesis, the arithmetic mean and standard deviation are calculated, and the significance of the differences for the expressions is tested through the chi-square test at a significant level of significance (5%), and the expressions are arranged according to their relative importance. Below are the results of the statistical analysis of the expressions of the first hypothesis, which measures the relationship between efficiency The effectiveness of internal auditing and enhancing cyber security**.**

Table No. (6) makes evident that:
1/The arithmetic mean for all statements of the first hypothesis is greater than the hypothetical means of the study according to the five-point Likert scale estimated (3). We also find that the level of significance for all statements is less than (0.05). The table also shows "the low dispersion in the responses of the study sample regarding all statements, through the values The standard deviation reflects the convergence in the views of the study sample members regarding all statements. This result indicates the sample members' agreement on the existence of a relationship between the efficiency and effectiveness of internal auditing and enhancing cyber security in the community that is the subject of the study, with a high degree of response, as all statements achieved an overall average of (4.17) with a standard deviation of (0.89).

2/It is noted from the table that the phrase (there is a commitment by the establishment to password policies) came in first place in terms of relative importance, as the average of the sample members' answers to the phrase was (4.23) with a standard deviation of (0.86). In the last place was the phrase (is carried out. Developing the team's capabilities and skills in terms of ingenuity, analysis, coding,

and digital intelligence), with an arithmetic mean (3.73) and a standard deviation (0.98).

Table No. (6): Results of the statistical analysis of the hypothesis of the first study

Statement	Mean	St. deviation	Level of Importance	chi-square	sig	Rank
Information security policies related to existing networks, database, and applications are applied .	3.90	0.80	High	28.4	0.001	1
Controls exist to prevent data loss and access to networks.	4.17	0.79	High	14.5	0.002	2
All tools and equipment purchased as cyber security supplies are actually used and not deposited in warehouses	3.97	0.85	High	12.4	0.006	3
Team abilities and skills are developed in terms of ingenuity Analysis Coding Digital Intelligence	3.73	0.98	High	26.7	0.001	4
There is a commitment by the facility to the password policies	4.23	0.86	V.high	16.1	0.001	5
There is a commitment by the facility to the policies of desktop computers and mobile phones	3.91	0.99	High	16.2	0.000	6
There is a commitment by the facility to the backup policies	4.10	0.88	High	11.3	0.010	7
total	4.17	0.89	High	17.9	0.000	

Source: The researcher conduction from field study 2024

3/The table shows the presence of statistically significant differences for all statements through the chi-square test for the significance of the differences, where the value of (chi-square) for the significance of the differences for all statements reached (17.9) with a significance level of (0.000), and this value is less than the significance level (0.05), and therefore this is It indicates that there are statistically significant differences in the answers of the sample members, in favor of those who agree with a high level of response to the total statements.

Based on the results of the statistical analysis shown in the previous paragraphs, the hypothesis of the first study is accepted, which states (the efficiency and effectiveness of internal auditing and enhancing cyber security) in all statements with a high level of response.

B. Presentation and analysis of the results related to the second hypothesis:

The second hypothesis states: (There is a statistically significant relationship between improving information security governance standards and reducing) electronic risks).

to verify the validity of the hypothesis, the arithmetic mean and standard deviation are calculated, and the significance of the differences for the statements is tested through the chi-square test at a significant level of significance (5%), and the statements are arranged according to their relative importance. Below are the results of the statistical analysis of the statements of the second hypothesis, which

measures the relationship between improving Information security governance standards and electronic risk reduction.

Table No. (7): Results of the statistical analysis of the second study hypothesis

Statement	Mean	St. deviation	Level of Importance	chi-square	sig	Rank
integrity of traditional and electronic documents isclosed and objective assurances are provided.	4.20	0.61	High	20.6	0.001	1
Digital assets are protected and the integrity of available data is ensured	4.13	0.90	High	35.3	0.001	2
The reliability and integrity of the required information is verified by the Board of Directors and the Audit Committee	4.10	0.76	High	17.2	0.001	3
ancial and operational reports are continuously ilable through official websites and electronic forms	3.23	1.14	medium	10.3	0.035	4
The facility's employees are trained and educated enough enough to enter and exit the network and retrieve information	3.87	0.94	High	8.1	0.042	5
Delivery processes for internal audit reports have been changed in line with the information age	3.77	0.77	High	17.7	0.001	6
rnal audit activities have been developed to vide projections on governance and risk nagement	3.93	0.94	High	17.8	0.001	7
total	3.89	0.87	High	18.1	0.000	

Source: The researcher conduction from field study 2024

Table 7 shows:

1. All of the first hypothesis's statements have an arithmetic mean that is higher than the study's hypothetical mean (3). Additionally, we discover that all of the claims have a significance level below (0.05). Additionally, the table displays "the low dispersion in the study sample's responses regarding all statements, as indicated by the standard deviation values, which demonstrate convergence." According to the study sample members' opinions of all statements, this result shows that there is a moderate degree of agreement among sample members regarding the relationship between raising information security governance standards and lowering electronic risks in the study's community.

This is because all statements received an average score of (3.89) overall, with a standard deviation of 0.87.

2. It is noted from the table that the phrase (the integrity of traditional and electronic documents is disclosed and objective assurances are provided about them) came in first place in terms of relative importance, as the average of the sample members' answers to the phrase was (4.20) with a standard deviation of (0.61). While the phrase was in last place (Financial and operational reports are made available on an ongoing basis through official websites and electronic platforms) with an arithmetic mean (3.23) and a standard deviation (1.14).

3.The table shows that there are statistically significant differences for all statements through the chi-square test for the significance of the differences, where the value of (chi) for the significance of the differences for all the statements reached (18.1) with a significance level of (0.000), and this value is less than the significance level (0.05), and therefore this indicates There were statistically significant differences in the responses of the sample members, in favor of those who agreed with a medium level of response to the statements that measured the hypothesis of the second study

Based on the results of the statistical analysis shown in the previous paragraphs, the hypothesis of the second study is accepted, which states (there is a statistically significant relationship between improving information security governance standards and reducing electronic risks) in all statements with a high response level.

Presentation and Analysis of Study Results

H1. The first hypothesis indicates a statistically significant relationship between the efficiency and effectiveness of internal audits and enhanced cybersecurity. Key findings include:

1. An overall average score of 4.17, indicating strong agreement on the relationship between internal auditing and cybersecurity.

2. The statement regarding commitment to password policies ranked highest, while the development of team capabilities ranked lowest.

H2. Analysis Related to the Second Hypothesis

The second hypothesis evaluates the link between improving information security governance standards and reducing electronic risks. Key findings include:

1. An overall mean of 3.89, reflecting moderate agreement on the impact of governance standards on electronic risk reduction.

2. The statement about the integrity of documents ranked highest, while the continuous availability of financial reports ranked lowest.

Conclusion

Both hypotheses are accepted, confirming significant relationships. The findings highlight the essential roles of internal auditing and information security governance in enhancing cybersecurity and mitigating risks.

Scientific Recommendations for Improvement

1. Enhance Training and Professional Development: Provide continuous training for internal auditors on the latest cybersecurity technologies and best practices.
2. Develop Information Security Governance Policies: Regularly review and update governance policies to align with global standards, including clear performance metrics and risk assessment procedures.
3. Implement Data Analytics Techniques: Use advanced data analytics to monitor unusual activities and proactively identify potential risks.
4. Enhance Communication Between Teams: Improve collaboration between internal audit teams, cybersecurity departments, and senior management to enhance security strategies and resource allocation

References

1. Abdel Aal, F. G. (2006). Requirements for activating the independence and impartiality of internal auditing in commercial banks in Egypt. *Journal of Business Studies and Research*.
2. Abdelazim, S. I., & Almarji, M. T. A. (2022, September). Internal auditors' role in risks related to outsourcing insurance: An exploratory study. *Alexandria Journal of Accounting Research*, 1-31.
3. Adel, A. A. (2022). The impact of internal audit quality in reducing cybersecurity risks and its repercussions on rationalizing investor decisions. *Journal of Financial and Business*.
4. Al-Sawalhi, A. (2024). Al-Rai Kuwaiti newspaper.
5. Al-Shawabkeh, A. A. (2019). The role of information security procedures in reducing information security risks at Taif University. *Studies and Research: The Arab Journal for Research and Studies in the Humanities and Social Sciences*, 1-69.
6. Attia, A. M. S. (2021). Does digital transformation in Egypt impose new responsibilities on auditors? *Business Research*, 53.
7. Abu Dhuwaib, Q. A. M. (2019). The extent of commitment to security policies and protection of accounting information in Jordanian commercial banks. *Jordan: Al-Bayt University, College of Graduate Studies*.
8. Bose, I., & Luo, J. (2014). Security investments and their impacts on organizational performance: A comprehensive framework. *Journal of Information Security*, 204-222.
9. Caliyurt, K., Bozkus, S., & Kahyaoglu, T. (2018). Cybersecurity assurance process from the internal audit perspective. *Managerial Auditing Journal*, 1-17.
10. Dawson, M. O. M., & Marwan, O. (2015). New threats and countermeasures in digital crime and cyber terrorism. *IGI Global*.
11. Elmaasrawy, H. E., & Tawfik, O. I. (2024). Impact of the assertive and advisory role of internal auditing on proactive measures to enhance cybersecurity: Evidence from GCC. *Journal of Science and Technology Policy Management*, ahead-of-print. https://doi.org/10.1108/JSTPM-01-2023-0004
12. Farah, N., Stafford, T. F., & Islam, M. S. (2018). Factors associated with security/cybersecurity audit by internal audit function: An international study. *Managerial Auditing Journal*, 377-409.

13. Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information Systems Security*, 5(4), 438-457.
14. Haapamäki, E., & Sihvonen, J. (2019). Cybersecurity in accounting research. *Managerial Auditing Journal*, 34(7), 808-834. https://doi.org/10.1108/MAJ-09-2018-2004
15. Hammad, T. A. (2007). Corporate governance concepts, principles, experiences, requirements. *Alexandria: Aldaar Aljamieiat Lilkutub*.
16. Hite, D. M., Schuessler, J. H., Prybutok, V., & Ramakrishnan, T. (2022). Work ethic and information security behavior. *Information and Computer Security*, 364-381.
17. Johari, A. F., & Hassan, T. M. T. (2019). Digital information security and ways to protect it in light of current legislation (pp. 1-58).
18. Kurniawan, Y., & Mulyawan, A. N. (2023). The role of external auditors in improving cybersecurity of the companies through internal control in financial reporting. *Journal of System and Management Sciences*, 13(1), 485-510. https://doi.org/10.33168/JSMS.2023.0126
19. Lau, L., Gan, H., & Yang, L. (2020). Investors' perceptions of the cybersecurity risk management reporting framework. *International Journal of Accounting & Information Management*, 1-17.
20. Lois, P., Drogalas, G., Karagiorgos, A., Thrassou, A., & Vrontis, D. (2021). Internal auditing and cyber security: Audit role and procedural contribution. *International Journal of Managerial and Financial Accounting*, 13, 25. https://doi.org/10.1504/IJMFA.2021.116207
21. Mahmoud, H. (2022, April 3). Electronic threats revive the cybersecurity industry: Trillion losses devastate the global economy. *Arab International Economic Newspaper*. https://www.aleqt.com/2022/04/03/article_2290841.html
22. Shehata, M. A. M. (2020). Measuring the impact of activating internal audit activities and digital transformation mechanisms on enhancing accountability and transparency and improving government performance. In *The Sixth International Conference for Environmental Studies and Research: Towards New Horizons for Sustainable Development* (p. 2).
23. Taha Hassan, T. M., & Johar, A. F. A. M. (2020). Security of digital information and ways to protect it in light of current legislation. *Egyptian Journal of Information Sciences*, 7, 161-222.
24. von Solms, B. (2001). Corporate governance and information security. *Computers & Security*, 215-218.
25. Hite, D. M., & Ramakrishnan, T. (2022). Work ethic and information security behavior.

دور المراجعة الداخلية في تعزيز الأمن السيبراني من وجهة نظر المراجعين

إيمان بابكر[1]
[1] أستاذ المحاسبة المساعد، كلية إدارة الأعمال - قسم المحاسبة - جامعة الأميرة نورة بنت عبد الرحمن، الرياض، المملكة العربية السعودية، iakhalid@pnu.edu.sa

الملخص
الهدف: تهدف هذه الدراسة إلى استكشاف دور إجراءات التدقيق الداخلي في تعزيز فعالية الأمن السيبراني. وتسعى للإجابة على أسئلة رئيسية: هل تشير كفاءة وفعالية التدقيق الداخلي إلى تطبيق معايير الأمن السيبراني بشكل صحيح؟ إلى أي مدى يمكن للجان التدقيق تحسين كفاءة التدقيق الداخلي وتحقيق أمن المعلومات؟ كيف تساعد معايير حوكمة أمن المعلومات في تقليل مخاطر الأمن السيبراني؟ للإجابة على هذه الأسئلة، تم مسح آراء 30 مدققًا داخليًا من السعودية والسودان ومصر.
المنهجية: تم استخدام المنهج الوصفي التحليلي.
النتائج: تشير النتائج إلى وجود علاقة إيجابية بين كفاءة وفعالية التدقيق الداخلي وتعزيز الأمن السيبراني. بشكل خاص، يرتبط نظام التدقيق الداخلي الأكثر فعالية بأمن معلومات أقوى، كما أن تحسين معايير حوكمة أمن المعلومات يقلل بشكل كبير من المخاطر الإلكترونية.
المساهمة والقيمة: تؤكد هذه الدراسة على الدور الحاسم للتدقيق الداخلي في تعزيز الأمن السيبراني من منظور المدققين، مع التركيز على تأثيره على أطر التدقيق واستراتيجيات الأمن. كواحدة من الدراسات القليلة التي تتناول هذا التقاطع، تقدم رؤى وتوصيات قيمة للمعنيين في كلا المجالين. تبرز الدراسة أهمية التدقيق الداخلي في حماية سرية المعلومات وتقليل المخاطر، وتقترح حلولًا مبتكرة تتماشى مع التطورات التكنولوجية لتعزيز القدرة على مواجهة الثغرات. في النهاية، تهدف الدراسة إلى تعزيز النقاش حول استراتيجيات إدارة المخاطر الفعالة في مشهد رقمي سريع التغير.

الكلمات المفتاحية: التدقيق الداخلي، الأمن السيبراني، مخاطر أمن المعلومات.