(Online) ISSN 2712-0554
Heritage and Sustainable Development *Original Research*
Vol. 7, No. 1, 2025, pp.317-328
https://doi.org/10.37868/hsd.v7i1.1130

The role of internal audit as a tool for enhancing cybersecurity effectiveness in Jordanian government agencies

Omar M. Alhawtmeh[1*]
[1] Department of Accounting, School of Business, University of Jordan, Aqaba, Jordan

*Corresponding author E-mail: a.alhawtmeh@ju.edu.jo

Received Feb. 13, 2025
Revised Apr. 1, 2025
Accepted Apr. 4, 2025
Online Apr. 16, 2025

Abstract
This paper investigates the role of internal audits as an instrument for enhancing the effectiveness of cyber security in Jordanian government agencies. To accomplish the study's objectives, a descriptive and analytical approach was used in analyzing whether the efficiency and effectiveness of IA directly influence cybersecurity standards. To investigate the research hypotheses, an analysis was conducted using linear equations utilizing SPSS software to perform statistical analysis and validate the findings. Additionally, a questionnaire was distributed to gather relevant data and provide further insights for the study. A structured questionnaire incorporating a five-point Likert scale was developed. Of the 100 questionnaires distributed, 84 were completed and returned for analysis. The research identified several key findings, with the greatest being the statistically significant influence of internal auditing on enhancing CS effectiveness and its subsequent effect on insurance costs.

Keywords: Audit, Internal audit, Cybersecurity, Effectiveness, Information security risks, Jordanian government agencies

1. Introduction

Internal audit is a critical component of organizational operations due to its pivotal role in identifying errors and minimizing their occurrence, as well as detecting weaknesses and implementing corrective measures. This process contributes to the establishment of a robust control system, enabling companies to realize their vision and achieve competitive advantages. Additionally, internal audit supports the development of stable frameworks that ensure the sustainability of business operations while fostering an environment conducive to organizational efficiency and growth.

Advancements in science and technology, coupled with the growth and diversification of company operations, have necessitated the development of control systems to assist management in ensuring the optimal utilization of resources, identifying potential deviations, and assessing the efficiency of ICS. The concept of IA has gained significance over time. Initially focused on examining an organization’s operations, records, and documents by an internal department, it has transformed into a broader function defined as an independent, objective assurance and a consultative activity focused on creating value and improving organizational operations. Although variations may influence the practice of internal auditing in different environments, adherence to the International Internal Audit Standards (IIA) is crucial for fulfilling the duties of IA and the auditing process [1].

In particular, Abu-Azza highlights that internal auditing adds value to the organization by providing services such as conducting OA and providing consulting on various management issues [2].

To address this, the International Auditing Standards Board introduced standards requiring public shareholding companies to establish audit committees. These committees play a key role in detecting errors, identifying weaknesses, and enhancing the performance of internal control systems while overseeing their operations. This requirement is reaffirmed in Article 21 of Chapter I of the Corporate Governance Rules Manual, which stipulates, "Boards of directors must implement measures to ensure internal control over the company's operations, including the establishment of a dedicated control unit." Internal auditing is responsible for ensuring compliance with applicable laws, regulatory requirements, internal regulations, and the policies, plans, and procedures set forth by the Board of Directors [3].

The infrastructure of government agencies is a vital national asset that is susceptible to cyber threats. Therefore, internal audit functions play a crucial role in identifying, assessing, and strengthening cybersecurity measures to safeguard sensitive data, operational systems, and regulatory compliance within Jordanian government agencies. This is achieved by identifying risks, evaluating controls, and ensuring adherence to regulatory standards. By promoting cybersecurity best practices, enhancing incident response preparedness, and cultivating a culture of vigilance, internal audits help protect critical infrastructure, ensure operational continuity, and secure sensitive information.

Internal audits provide a crucial framework for managing and mitigating cyber risks, helping Jordanian government agencies maintain resilience in a rapidly evolving digital landscape. They enable agencies to perform risk-based assessments, identifying the most critical cybersecurity threats, such as unauthorized access, data breaches, and ransomware attacks. Auditors uncover vulnerabilities in systems, networks, and processes, prioritizing those that pose the highest risk to sensitive government operations and citizens' data. In addition, auditors assess cybersecurity policies and procedures, ensuring they are up-to-date, properly implemented, and adhered to across all departments while also identifying any gaps that need to be addressed.

Over the past few years, CS has become one of the most pressing risk management challenges for organizations across various sectors. For instance, previously, the International Auditing Framework was updated to address the growing role of information technology across all areas of business operations [4]. Based on this context, the researcher argues that it is crucial to investigate the state of cybersecurity within Jordanian government agencies, as their importance directly influences the national economy and society. The study seeks to know how internal audits enhance cybersecurity in Jordanian government agencies. From the previous we can derive the study hypotheses as follows:

H1: Internal auditing contributes to enhancing the effectiveness of cybersecurity in Jordanian government agencies

H2: There is a complementary relationship between IA and cybersecurity insurance cost in Jordanian government agencies.

H3: Internal auditing works to identify the strengths and weaknesses in the system of cybersecurity.

1.1. Conceptual and theoretical overview

Cybersecurity is a vast and essential field that focuses on protecting systems, networks, and data from cyber threats and unauthorized access. CS encompasses different topics and specialties, such as Network Security, Application Security, Information Security, Operational Security, Enterprise Security, Incident Response and Recovery, Ethical Hacking and Penetration Testing.

IA actively contributes to driving digital value by identifying risks and offering strategic guidance [5]. Achieving adequate and effective IA standards is essential. The originality of this paper stems from highlighting the significance of adapting IAS for performance and their role in enhancing organizational evaluating [6]. The extent of cybersecurity audits by internal auditors is highly and positively correlated efficiently with the internal auditor in relation to governance, risk, and control [7].

Bou-Raad states that the role of IA is included from a traditional audit to a more proactive, value-driven function, with auditors increasingly collaborating with management as strategic partners with visible examples emerging. IA are embracing change to meet market demands, aiming to provide valuable services to the organizations they serve [8]. Governments and individuals can use cybersecurity as a strategic weapon, particularly as cyber warfare is now a fundamental component of contemporary attack and warfare strategies [9].

Cybersecurity has indeed become a cornerstone of national security policies worldwide. With the rapid digitization of critical infrastructure, government systems, financial networks, and communications, nations are increasingly prioritizing measures to safeguard their digital ecosystems against cyber threats such as cyber-attacks on critical infrastructure, state-sponsored cyber espionage, ransomware, and financial crimes. In response to these challenges, many countries have developed comprehensive legislation aimed at safeguarding information security, thereby reinforcing their commitment to the protection of personal and institutional data.

Managers should recognize internal audits as a crucial element in mitigating cybersecurity risks and enhancing proactive measures [10].

Focusing on the Jordanian government, recent studies have examined internal audits within government agencies as tools for enhancing cybersecurity. These investigations show that organizational culture, resource allocation, and legislative frameworks significantly influence the efficiency of internal audits in addressing cybersecurity challenges in the government sector.

Different studies examined internal audits within government agencies as tools for enhancing cybersecurity such as Al Barzngi emphasizes the need for internal auditors to be granted adequate authority, the importance of updating internal audit approaches annually and flexibly on a risk-based basis using appropriate methodologies, and the strengthening of collaborative relationships between the internal audit role and technical aspects departments such as information technology and cybersecurity to enhance cybersecurity across economic entities [11].

Ghelani explores the extensive security guidance found in both academic and professional literature. While strategies like deterrence, deception, detection, and response are available, most research primarily emphasizes technological countermeasures for threat prevention [12]. The findings suggest that many organizations primarily adopt a preventive approach to ensure the availability of technology services, with other identified strategies supporting this preventive focus at the operational level.

On the other hand, Usman et al. in this sector face numerous challenges, prompting organizations to strategically implement measures to protect integrity, confidentiality, and availability of information. Furthermore, innovation introduces a variety of risks and threats to the IA within these organizations [13].

Alhawtmeh employed statistical tools. The overall indication is that Jordanian companies do not fully adhere to IIAS. Instead, they follow practices dictated by government rules and guidelines, which are not entirely aligned with international standards. Consequently, the results suggest a weak commitment to these essential standards within the sampled companies. Based on these findings, the researchers provide several recommendations aimed at achieving more effective adoption of IAS [14]. There is a relationship between internal audit (IA) and the internal control (IC) system, which is described below. The internal auditor operates within an economic unit; it is evident that their role is to support management through the control process. Thus, the internal auditor's focus on the control process can be outlined as follows:

1. IA helps the unit achieve effective internal control as well as encourage continuous improvement of the control process as the audit outputs are considered inputs to the internal control system.
2. The administrative function comprises several sub-functions, including planning, organizing, directing, supervising, and monitoring, which form the core of control activities. Internal audit is instrumental in supporting the execution of these functions.

3. The independence of the audit from the operational processes within the unit enhances the internal audit's ability to assess the level of confidence in performance. This, in turn, allows the control system to realign actual performance with planned performance, thereby ensuring effective control.
4. Since internal auditing is considered one of the systems within the unit, its proximity to the accounting systems makes it aware of the issues facing the unit. This drives it to understand the operational processes carried out by these systems to enhance knowledge and complete the control process.
5. Internal auditing provides a continuous review and assessment of the systems and procedures established by management, aimed at enabling internal control to effectively monitor the unit's activities.
6. Risk management processes can be enhanced through the key roles of internal auditing, as there is an important relationship between risk management and internal auditing.

Some challenges facing the Internal Audit Function in Jordanian Government Agencies Despite the critical role of internal audit, obstacles persist. These include:

- Insufficient resources and budget for comprehensive audits
- A scarcity of cybersecurity-trained auditors
- Resistance to change among staff and management
- The ever-evolving nature of cyber threats, requiring constant adaptation

The research model developed by the author is shown below in Figure 1.

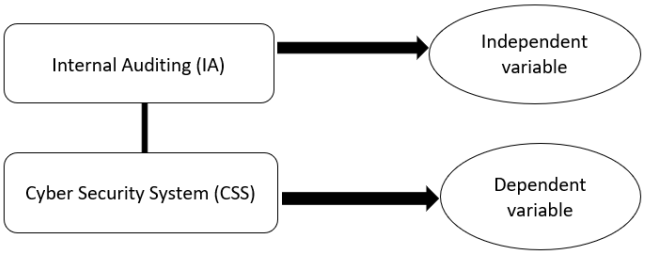

Figure 1. Research model

2. Research method

2.1. Research design and data collection

A descriptive and analytical approach was used in analyzing whether the efficiency and effectiveness of IA directly influence cybersecurity standards. Financial data analysis conducted using linear equations utilizing SPSS software to perform statistical analysis and validate the findings. Additionally, a questionnaire was distributed to gather relevant data and provide further insights for the study. A structured questionnaire incorporating a five-point Likert scale was developed.

This study employed both primary and secondary data collection methods to investigate the role of internal auditing in enhancing cybersecurity effectiveness in Jordanian government agencies. The primary data was gathered through a structured questionnaire specifically designed to measure key constructs, including internal auditing practices, cybersecurity effectiveness, cyber insurance costs, and the identification of cybersecurity system strengths and weaknesses. The questionnaire was developed based on insights from existing literature and international internal audit standards and was structured using a five-point Likert scale, ranging from “Strongly Disagree” (1) to “Strongly Agree” (5). A purposive sampling technique was adopted to target individuals working in internal audit or cybersecurity roles within various Jordanian government institutions.

A total of 100 questionnaires were distributed across relevant ministries and public sector agencies. Of these, 84 completed questionnaires were returned and considered valid for analysis, yielding a response rate of 84%. This high response rate ensured an adequate representation of the target population for the purposes of statistical analysis. Secondary data was also reviewed to support the conceptual framework and hypotheses development. These sources included prior academic studies, internal audit standards issued by professional organizations

such as the Institute of Internal Auditors (IIA), government guidelines, and reports on public sector cybersecurity. Ethical protocols were followed throughout the data collection process. Participants were informed of the voluntary nature of their involvement, assured of confidentiality, and consented to the use of their responses solely for research purposes.

2.2. Data Analysis

Following data collection, the Statistical Package for the Social Sciences (SPSS) was used to conduct comprehensive data analysis. The analysis involved multiple steps to validate the data and test the study's hypotheses. Initially, descriptive statistics were used to summarize demographic characteristics and key variables, offering a general understanding of respondent profiles and response distributions. Next, reliability analysis was conducted using Cronbach's Alpha to assess the internal consistency of the questionnaire scales. The reliability scores confirmed the suitability of the instrument for further statistical testing. To examine the hypothesized relationships, multiple linear regression analysis was employed. This method assessed the impact of internal auditing (independent variable) on three dependent variables:

1. Cybersecurity effectiveness,
2. Cyber insurance cost, and
3. Identification of strengths and weaknesses in the cybersecurity system.

To test the first hypothesis, the following linear regression model was developed:

$CS = B_0 + B_1 IA + E$

where, IA is independent variable, CS is intermediate variable (CS effectiveness), E is estimation errors or statistical residuals, B_0 is regression equation constant, represents the value of the dependent variable when the value of the independent variable is equal to zero, B_1 = regression function slope, measures the impact of the independent variable on the dependent variable.

H2: There is a complementary relationship between internal auditing and the effectiveness of the cybersecurity in Jordanian government agencies.

To test the second hypothesis, the following linear regression model was developed:

$IC = B_0 + B_1 CS + E$

where, IC is Cyber insurance cost.

H3: Internal auditing works to identify the strengths and weaknesses in the system of cybersecurity.

To test the third hypothesis, the following linear regression model was developed:

$IC = B_0 + B_1 IA + E$

Each regression model was evaluated based on key indicators, including:

- Correlation coefficients (R) to determine the strength of relationships,
- Coefficient of determination (R^2) to assess the proportion of variance explained,
- ANOVA (F-tests) to test the overall model significance,
- T-tests and significance levels (p-values) to determine the individual predictive power of independent variables,
- Standard errors to gauge the precision of the estimators,
- P-P plots and residual analyses to ensure the assumptions of normality and linearity were met.

The analysis revealed statistically significant and strong positive relationships between internal auditing and each of the dependent variables. These results confirmed all three hypotheses, indicating that internal audit plays a crucial role in improving cybersecurity effectiveness, reducing associated insurance costs, and identifying systemic vulnerabilities in cybersecurity frameworks within Jordanian government agencies.

3. Results and discussion

H1: Internal auditing contributes to enhancing the effectiveness of the cybersecurity in Jordanian government agencies.

After testing the developed equation, the correlation coefficient (R) between the variables is 0.881, indicating a strong relationship. The determination coefficient (R^2) is 0.776, which reflects the explanatory power of the hypothesis. Specifically, the independent variable (internal audit) accounts for 88.1% of the variance in the intermediate variable (CS effectiveness). Additionally, the estimated standard error (Estimate Std. Error) is 0.1440, which is a relatively low value, suggesting minimal estimation error. A lower standard error indicates a higher level of statistical accuracy (Table 1).

Table 1. H1 test results

Model (M)	R	R^2	Adjusted R^2	Std. Error of the Estimate
1	0.881	0.776	0.772	0.144

The results of an ANOVA test, where the computed F-value is 265.4, Sig. surpassing the critical value of 3.69, based on degrees of freedom (df = 81, 3) at a 5% significance level. Additionally, the sig. level is 0.00, which is well below the commonly accepted threshold of 0.05, indicating a highly significant result in the context of social science research (Table 2).

Table 2. Variance in first hypothesis testing

M		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	6.901	3	2.3003	265.4	0.00
	Residual	2.768	81	0.0342		
	Total	9.669	84			

The regression equation coefficients have the constant (B0) value of 0.581 and the slope (B1) value of 0.826. These values illustrate the relationship between the independent variable and the intervening variable, as indicated by the coefficient B. The positive value of B1 suggests a direct relationship between the independent variable (internal auditing) and the intervening variable (CS effectiveness). Specifically, for every one-unit increase in internal auditing, there is a corresponding 82.6% increase in CS effectiveness, which has emerged as a crucial mediating factor in analyzing various independent variables in social phenomena. Furthermore, when evaluating the statistical significance of the relationship between the independent variables and CS effectiveness, the t-statistic for the independent variable is recorded at 0.00. This value is significantly lower than the conventional threshold of 0.05, indicating that the sample data provides strong evidence to reject the null hypothesis and accept the alternative hypothesis, thereby confirming the existence of a statistically significant effect.

Table 3. Regression analysis - "Internal auditing contributes to enhancing the effectiveness of cybersecurity in Jordanian government agencies"

M		Unstandardized Coefficients		Standardized Coefficients	T	Sig.
		B	Std. Error	Beta		
1	Constant	0.581	0.233		2.331	0.011
	Audit focus	0.826	0.053	0.824	15.827	0.000

The regression equation that was used to test the hypothesis can be reformulated based on the results obtained to become:

CS= 0.5+0.83*IA

The strong relationship between the two variables is represented by the curve in Figure 2.

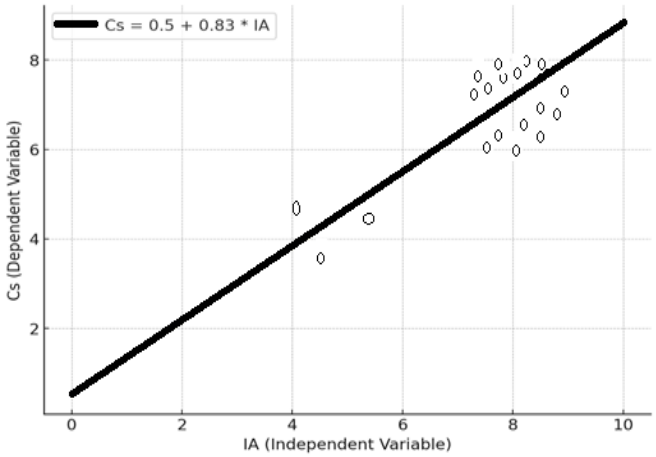

Figure 2. Linear relationship between CS and IA

The conditions for conducting the regression analysis test are fulfilled, as shown by the alignment of points along the straight line. This suggests that the statistical residuals follow a normal distribution in Figure 3.

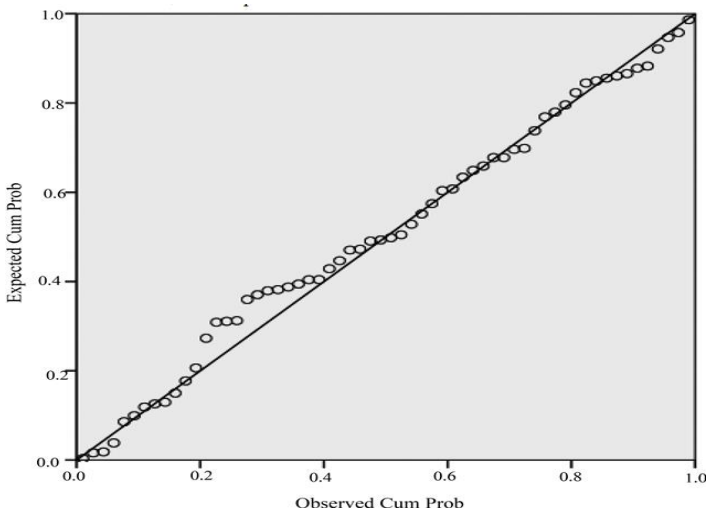

Figure 3. Normality P-P plot of regression standardized residual dependent variable CS

H2: There is a complementary relationship between internal auditing and the effectiveness of the cybersecurity in Jordanian government agencies.

After testing the hypothesis the correlation coefficient (R) between the variables is 0.788, indicating a strong relationship, while the coefficient of determination (R^2) is 0.621, reflecting the "explanatory power" of the hypothesis. This means the independent variable (internal audit) accounts for 78.8% of the variance in the intermediate variable (CS effectiveness). Additionally, the standard error of the estimate (Std. Error of the Estimate) is 0.1680, which is relatively low. A smaller standard error indicates higher statistical accuracy (Table 4).

Table 4. Correlation coefficient

M	R	R^2	Adjusted R^2	Std. Error of the Estimate
1	0.788	0.621	0.620	0.168

The results of an ANOVA test, with the computed F-value of 235.6, greatly surpasses the critical value of 3.69, based on degrees of freedom (df = 81, 3) at a 5% Sig. level. Additionally, the level (Sig) is reported as 0.000, which is significantly lower than the acceptable error rate of 0.05 commonly used in social science research (Table 5).

Table 5. Variance in second hypothesis testing (dependent variable IC)

M		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	7.803	3	2.601	235.6	0.00
	Residual	2.886	81	0.0348		
	Total	10.689	84			

The constant value in the regression equation, B0, is 0.453, while the slope value, B1, is 0.922. These values demonstrate the relationship between the independent variable and the intervening variable, as reflected by the coefficient B. The positive value of B1 suggests a direct relationship between the independent and intervening variables. Specifically, for every one-unit increase in the independent variable, which is internal auditing, there is a corresponding 85.5% increase in the intervening variable, CS effectiveness, which has emerged as a critical concern and functions as a mediating variable amidst various independent factors in the analysis of social phenomena. Moreover, when assessing the statistical significance of the relationship between the independent variables and CS effectiveness, the t-statistic for the independent variable is found to be 0.00, as shown in the table. This value is significantly lower than the predetermined error threshold of 0.05 in social sciences, providing strong evidence to reject the null hypothesis and accept the alternative hypothesis, thus confirming the presence of a statistically significant effect: “There is a complementary relationship between IA and the CS insurance cost in Jordanian government agencies (Table 6).

Table 6. Regression analysis (dependent variable IC)

M		Unstandardized Coefficients		Standardized Coefficients	T	Sig.
		B	Std. Error	Beta		
1	Constant	0.453	0.242		1.821	0.174
	CS	0.922	0.051	0.855	15.652	0.000

The regression equation that was used to test the hypothesis can be reformulated based on the results obtained to become:

IC= 0.45+0.92*CS

The strong correlation between the two variables is shown by the curve in Figure 4.

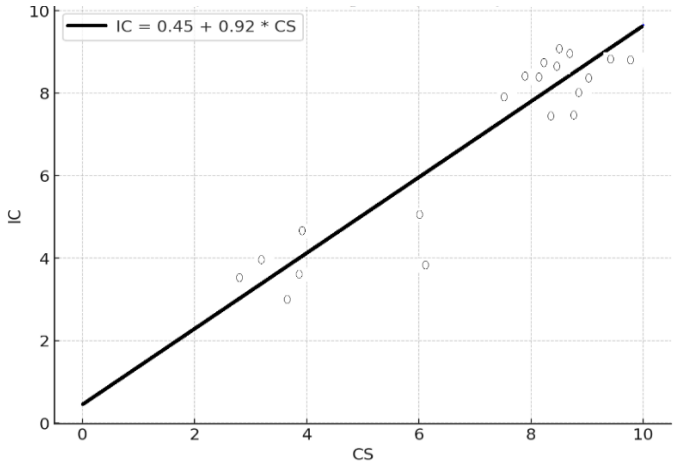

Figure 4. Linear relationship between CS and IC

The conditions for the regression analysis test are satisfied, as depicted graphically by the distribution of points around the straight line. This indicates that the statistical residuals follow a normal distribution Figure 5.

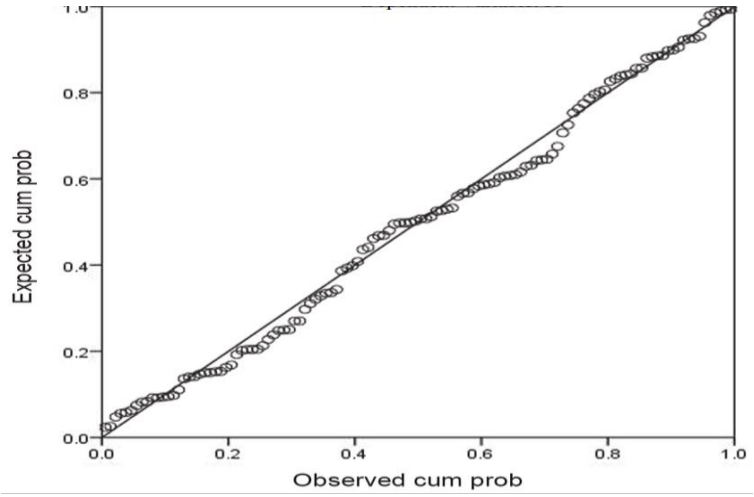

Figure 5. Normality P-P plot of regression standardized residual dependent variable IC

H3: Internal auditing works to identify the strengths and weaknesses in the system of cybersecurity.

After testing hypothesis the correlation value (R) between the variables is 0.857, indicating a strong relationship, while the coefficient of determination (R^2) is 0.734, reflecting the "explanatory power" of the hypothesis. This means that the independent variable (IA) accounts for 73.4% of the variance in the intermediate variable (CS strengths and weaknesses of the CS system). Furthermore, the standard error of the estimate is 0.1880, which is quite low. A lower standard error indicates greater statistical accuracy (Table 7).

Table 7. Summary of the model for testing the third sub-hypothesis

M	R	R^2	Adjusted R^2	Std. Error of the Estimate
1	0.857	0.734	0.732	0.188

The results of an ANOVA test, with the computed F-value of 228.91, significantly surpasses the critical value of 3.69, based on degrees of freedom (df = 81, 3) at a 5% Sig level. Additionally, the significance level is reported as 0.000, well below the predetermined acceptable error rate of 0.05 in social science research (Table 8).

Table 8. Variance in third hypothesis testing (dependent variable IC)

M		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	8.109	3	2.703	228.91	0.00
	Residual	2.934	81	0.0362		
	Total	11.042	84			

The constant value in the regression equation, B0, is 0.410, while the slope value, B1, is 0.912. These values represent the relationship between the independent and intervening variables, as indicated by the coefficient B. The positive value of B1 suggests a direct or positive relationship between the independent and intervening variables. Specifically, for every one-unit increase in the independent variable—internal auditing—there is a corresponding 85.7% increase in the intervening variable, which represents the strength or weakness of the cybersecurity system. This variable has emerged as a critical concern, acting as a mediating factor amidst various independent variables in the analysis of social phenomena. Furthermore, when assessing the statistical significance of the relationship between the independent variables and cybersecurity effectiveness, the t-statistic for the independent variable is recorded at 0.00, which is substantially lower than the acceptable error threshold of 0.05 commonly used in social science research. This result provides strong evidence to reject the null hypothesis and accept the alternative hypothesis, confirming the presence of a statistically significant effect for the third hypothesis: “Internal auditing works to identify the strengths and weaknesses in the system of cybersecurity” (Table 9).

Table 9. Regression analysis (dependent variable IC)

M		Unstandardized Coefficients		Standardized Coefficients	T	Sig.
		B	Std. Error	Beta		
1	Constant	0.410	0.262		1.621	0.124
	CS	0.912	0.061	0.857	15.147	0.000

The regression equation that was used to test the hypothesis can be reformulated based on the results obtained to become:

IC= 0.41+0.91*IA

The strong correlation between the two variables is represented by the curve in Figure 6.

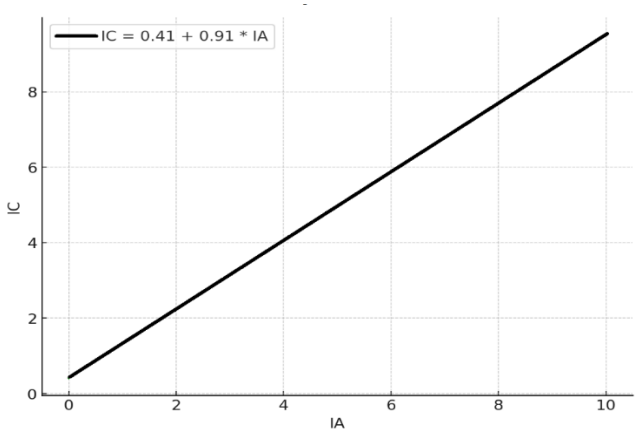

Figure 6. Linear relationship between IA and IC

The conditions for the regression analysis test are satisfied, as shown by the distribution of points around the straight line. This confirms that the statistical residuals follow a normal distribution Figure 7.

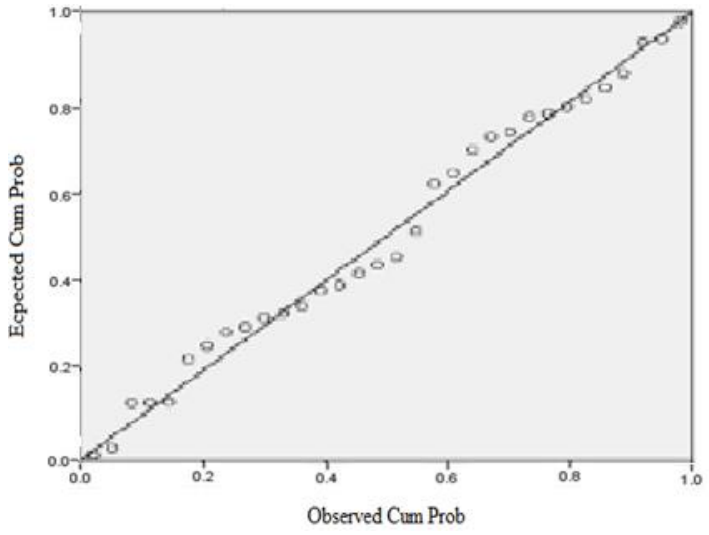

Figure 7. Normality P-P plot of regression standardized residual dependent variable IC

4. Conclusions

This paper concludes with testing and assessing controls, identifying security gaps, compliance monitoring, raising awareness, and recommending improvements. Internal auditing makes it possible in light of changing economic conditions. Internal auditing is considered a specialized body within the economic unit that conducts evaluations, and what distinguishes it from other functions is its independence. The management of economic units needs internal auditing as a decisive tool to monitor the extent of implementation of its policies and

procedures, and every aspect of it must be covered. Operations of economic units through the internal audit process.

The study hypothesis test clarifies that internal auditing contributes to enhancing the effectiveness of cybersecurity in Jordanian government agencies, and there is a complementary relationship between IA and the CS insurance cost in Jordanian government agencies. In addition, internal auditing works to identify the strengths and weaknesses in the system of cybersecurity.

The study recommended that it is necessary to develop ongoing training programs for employees at all levels, emphasizing the introduction to their roles and responsibilities. The rewards for adhering to regulations and Instructions, correct behavior, and the penalties for violating them. The ethical and humanitarian aspects of the profession must also be covered in these courses.

Summits should be devoted to information security and protection, the goal of which is to monitor and update information security and protection programs, administrative systems, and technical devices, coming from the belief that cybersecurity is the best and fastest way to protect data and systems.

Declaration of competing interest

The author declares that they have no known financial or non-financial competing interests in any material discussed in this paper.

Funding information

No funding was received from any financial organization to conduct this research.

Author contribution

The contribution to the paper is as follows: O. M. Alhawtmeh: study design, developed the methodology and data analysis, interpreted the results and wrote the paper, draft final preparation. The author approved the final version of the manuscript.

References

[1] J. W. Gunther and R. R. Moore, "Auditing and auditors: Oversight or overkill?" Federal Reserve Bank of Dallas," *Economic and Financial Policy Review*, vol. 1, no. 5, pp. 76–91, 2002.

[2] W. Abu-Azza, "Perceived effectiveness of the internal audit function in Libya: A qualitative study using institutional and Marxist theories," Ph.D. dissertation, University of Southern Queensland, 2012.

[3] Securities Commission, "Guide to governance rules for public joint-stock companies listed on the Amman Stock Exchange," Amman, Jordan, 2227. http://jsc.gov.jo/library/633571467958396032.pdf.

[4] E. Haapamäki and J. Sihvonen, "Cybersecurity in accounting research," *Managerial Auditing Journal*, vol. 34, no. 7, pp. 808–834, 2019. https://doi.org/10.1108/MAJ-09-2018-2004.

[5] M. A. M. Shehata, "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, 2020.

[6] O. M. Alhawtmeh, M. Aladwan, and A. Alkurdi, "Internal audit practices consistency with international internal auditing standards for entities with government contribution," *Italian Journal of Pure and Applied Mathematics*, no. 47, pp. 182–204, 2022.

[7] N. Farah, T. F. Stafford, and M. S. Islam, "Factors associated with security/cybersecurity audit by internal audit function: An international study," *Managerial Auditing Journal*, vol. 33, no. 4, pp. 377–409, 2018.

[8] G. Bou-Raad, "Internal auditors and a value-added approach: The new business regime," *Managerial Auditing Journal*, vol. 15, no. 4, pp. 182–187, 2000.

[9] A. Al-Sawalhi, "*Al-Rai Kuwaiti newspaper*," 2024.

[10] H. E. Elmaasrawy and O. I. Tawfik, "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, 2024. https://doi.org/10.1108/JSTPM-01-2023-0004.

[11] S. Al Barzngi and Z. Alsaqaa, "Internal audit requirements to enhance cybersecurity in economic units considering the Institute of Internal Auditors (IIA) guidelines," *Tikrit Journal of Administrative and Economic Sciences*, vol. 20, no. 67, 2023.

[12] G. Drogalas, T. Karagiorgos, and K. Arampatzis, "Factors associated with internal audit effectiveness: Evidence from Greece," *Journal of Accounting and Taxation*, vol. 7, no. 7, pp. 113–122, 2015.

[13] A. Usman Alih, A. Ahmad, and S. O. Abdulmalik, "Cybersecurity risk assessment and the role of internal audit function among the listed financial companies in Nigeria: A global empirical perspective," *Creative Journal of Business Research*, vol. 1, no. 1, 2023.

[14] O. M. Alhawtmeh, "Governments' investments commitment to internal audit requirements: The case of Jordan," *International Journal of Accounting, Auditing and Performance Evaluation*, vol. 18, no. 3–4, 2023.