Journal of Research Administration
Society of Research Administrators International

THE IMPACT OF THE INTERNAL AUDIT DEPARTMENT IN EVALUATING AND MANAGING CYBER SECURITY RISKS AND THE MEDIATING ROLE OF INSTITUTIONAL CULTURE IN BANKS OPERATING IN JORDAN

Ola Muhammad Khresat

Associate professor, Zarqa University, P.O.Box: 132222-zarqa 13132-jordan

Abstract:

The study aimed to demonstrate the impact of the internal audit department in assessing and managing cyber security risks in Jordanian commercial banks and the mediating role of institutional culture. The study relied on the descriptive method in analyzing the data. To achieve the objectives of the study, a questionnaire was prepared, 140 of which were distributed to commercial banks operating in Jordan, and 120 questionnaires were retrieved. To measure the variables of the study, a five-point Likert scale was used, and to test mediation, the Baron & Kenny model was used. After testing the hypotheses, it was found that the internal audit department has a direct impact on the institutional culture and on cyber security risk assessment and management in the regression model. It was also found that there is an effect of institutional culture on risk assessment. “Cyber security and its management,” but when mediated by institutional culture, the internal audit department does not predict the assessment of cyber security risks and their management, and this is considered an indirect effect. Therefore, the study recommends that internal audit departments acquire the skills that enable them to carry out internal audit operations using methods based on modern technology in light of Cyber security threats

JEL: M410, M420, M480, G240,
Keywords: Internal Audit Management, Cyber security Risk Assessment and Management, Corporate Culture, Institutional culture, banks operating in Jordan.

i. INTRODUCTION

In light of the digital business environment, which revolves directly in the so-called electronic network or cyberspace, and what this entails in adopting countries and institutions in executing most of their work on digital computers and storing their data on electronic networks and in the electronic cloud, which achieves for countries and institutions more efficiency in managing And it makes those countries and institutions obligated to maintain a safe digital environment within this cyberspace, which forces companies to pay attention to cyber security (Kahyaoglu and Caliyurt, 2018).

Hence, cyber security has become an indispensable requirement, especially with the emergence of asymmetrical or asymmetrical challenges that do not recognize international or national borders or sovereignty and that do not recognize patents or intellectual property. Cyber security protects countries and institutions from risks coming from external sources. Through the Internet, in other words, it protects computers, servers, and places where information is stored from any cyber

attacks, which may pose a risk to the security of those computers and servers and the important and sensitive information they contain for those countries and institutions, and these risks and threats may come in several forms, such as Spreading viruses, copying confidential and important information, modifying and distorting it, or adding incorrect information on important sites, and here comes the role of cyber security in protecting that information from distortion, alteration, and forgery. (Almarat and Hamamsa 2022)

This coincided with the expansion and increase in internal audit tasks. The work of the internal auditor is no longer limited to checking documents and papers, but enumerates them, so that it includes evaluating and judging the adequacy of institutional culture systems in preventing and limiting abuses that may occur in institutions and the most important of these challenges are security challenges. Cyber security, which has become the most dangerous threat facing the internal auditors community, in light of the occurrence of about two billion cyber attacks per day, as mentioned at the 19th annual regional conference of internal auditing held in Abu Dhabi, or in judging the organizational culture systems that are based on limiting or even preventing Any risks related to cyber security by examining cyber control systems and providing a clear vision for senior management to develop a comprehensive internal audit plan that addresses all aspects related to cyber security. (Amirhom 2022).

This requires internal audit departments to pay attention to matters of competence and professionalism in order to develop a department that is able to keep pace with these dangerous developments in the digital environment represented by the risks and threats contained in cyberspace, they must develop their skills related to modern technology and be sufficiently aware of the risks related to it and acquire the skills that enable them to carry out internal audits using methods based on modern technology (Islam et al., 2018)

Perhaps one of the most important things that must be included in the culture of any institution within its ethical, value or cultural organization is the culture of cyber security that makes it the objectives of the institution to maintain the confidentiality and protection of information.

Hence, this study came to show the impact of the Internal Audit Department in assessing and managing cyber security risks and the mediating role of institutional culture in banks operating in Jordan.

Study importance:

• The study lies in the importance of internal audit management in assessing and managing cyber security risks.

• Demonstrate the importance of institutional culture in compliance with cyber security controls to protect information and confidentiality and mediate the relationship between the internal audit department and the assessment and management of cyber security risks.

ii. Theoretical framework

Many books and researches have dealt with the terminological meaning of cybersecurity, as (Al-Amarat and Al-Hamasa 2022) defined it as "a set of mechanisms, procedures, means, and frameworks that aim to protect software and computers from various attacks, penetrations, and

cyber threats that may threaten the national security of states" in When the report issued by the International Telecommunication Union in the framework of its discussion of the trends of reform in telecommunications for the year 2014-2015 defined cyber security as “the set of tasks such as the collection of means, policies, security procedures, guidelines, risk management comparisons, trainings, best practices and techniques that can be used to protect the environment.” Cyber assets, organizations and users.

So, cyber security aims by taking measures, means and procedures to protect the property of companies and countries from software and information that may affect the national security of the state or information those companies consider strategic for their survival from attacks that aim to steal this information.

Hence, the importance of cybersecurity in protecting this information from the risks caused by cyber attacks and crimes, and cyber attacks or what some like to call cyberspace or cyber warfare, and according to what many studies have indicated that there are many types of cyber risks, according to a study (shahimi & Mahazan 2018) and a study (He, et, al, 2018c), there are three types of cyberattacks, which are 1- Risks related to confidentiality and occur when there is a breach of systems and information or when sharing this information with a third party 2- Integrity risks in case of fraud and abuse of systems 3- Risks related to continuity in the event of business interruption or disruption for other reasons. Through reviewing the above, it becomes clear how important and dangerous cybersecurity issues are, and many questions arise about the role of states, organizations, regulatory bodies, legal auditors, control and internal audit bodies and sections in reducing the risks of these threats. During the identification of the gap between the existing situation and the desired situation, identifying weaknesses, reviewing new technology and its new risks, must be guarded against, and reviewing deep technology by assessing the security risks involved in advanced technology and the need for a comprehensive understanding of it.

According to the Committee of Principles of Sound Risk Management issued in 2019 by (Committee of sponsoring organizations of the tread way commission), there are three lines of defense for cyber security, the first consists of managers of business units in conjunction with the information technology function, where they take all the necessary measures, means and procedures to protect their organizations from cyber security risks, and the second consists of information security risk management through the availability of the necessary expertise to implement and effectively cyber security controls, while the line third of defense is the Internal Audit Department, which performs the audit and review function, where it reports to senior management on the adequacy of procedures, policies, controls and strategies related to protection from cyber attacks, including assessing the adequacy of actions and means related to the first and second lines of defense (IIA, 2020, coso, 2019 (Slapnicar, 2022, Vuko et al., 2021).

In another context, the IIA report (2022) indicated that the problem of cybersecurity ranges from accountability to multiple parties, and internal audit can achieve balance and help determine accountability through assurance and counseling services, and internal audit can provide its vision

regarding the potential for increasing risks of data breaches and breaches. Security resulting from easing the matter of increasing regulatory controls, and it can also work to assess awareness of cybersecurity and the adequacy of training programs for employees in light of the information technology environment in addition to its contribution to improving companies' understanding of cyber security risks and identifying possible strategies to mitigate these risks and the effectiveness of cybersecurity risk management . (2020, KPMG).

This leads us to talk about the culture of the institution and its view of the importance of cybersecurity and reducing its risks, the institutional culture has an important impact on directing work and activities of institutions and according to the researcher's point of view, institutional culture is the standards of behavior within the institution determined by common values and rules of conduct and this culture was formed throughout the institution's history life and formed its distinctive character in dealing with the internal and external pressures and risks it is exposed to, and in this regard, Jordan was the first Arab country Which developed a national strategy for cybersecurity in 2012, where the Central Bank developed the infrastructure of the financial sector, including electronic payment systems, by providing digital financial services, if it reached approximately 14 billion Jordanian dinars during the years 2020 and 2021In this regard, the Jordanian banking sector realized the importance of cybersecurity and its various dimensions on banks, as banks have made achievements to enhance cyber security to reach the levels highest of safety In this regard, the Central Bank of Jordan issued the cybersecurity framework in the banking sector in mid-2021, and the Central Bank issued a set of instructions, circulars and supervisory guides aimed at enhancing cybersecurity in the financial and banking sector (FINCERT) and aims to enhance the readiness and ability of the banking sector to face and respond to cyber risks. The Central Bank of Jordan has a special unit to respond to cyber incidents for the financial and banking sector in partnership with the banking sector, where the unit began to develop governance frameworks, policies and instructions necessary to strengthen the cybersecurity system for the institutions of the banking and financial sector in order to enhance the readiness of the banking sector to face cyber risks to reach the development and implementation of security programs and standards to evaluate the effectiveness and efficiency of cyber security controls and measure the maturity level of each institution.

iii. Previous studies:

Many studies dealt with cyber security topics and the role of internal audit and audit in contributing to reducing cyber security risks, including a study (Sergeja 2022,Alina,et,al2017,, Islam,,etal,2018), where the results confirmed that internal audit departments play a key role in reducing cyber security risks and in the cyber security audit process and that they contribute effectively to achieving information security, governance, risk management and management provision. Reports showing the adequacy of the strategies and policies followed by the various departments in reducing cyber security risks and that judging the efficiency of internal audit departments depends on the legislation, standards and organizational characteristics of the

institution, and that especially investors and stakeholders,, will not be able to follow up cyber risk operations without the help of departments that managed internal audit and audit. The Vuko 2021 study found that the testimonies and experiences of internal auditors regarding cyber security constitute strong evidence of the effectiveness of cyber security-related audits. The study of Lios, et, al 2020, Shamsuddin, 2018, Salah, 2022 agreed with it. To examine the variables that affect cyber security and that are related to internal audit, and the studies have identified the variables of the advisory role and cooperation between the information technology specialist and the internal auditor, technological knowledge, policies, standards, information and staff training with regard to information technology, and the studies have concluded that the relationship between IT specialists and internal auditors is very limited, in addition, the level of specialized technological knowledge on the part of internal auditors is low with regard to the standards of cyber security policies that Reviewed by the internal auditor, the internal auditors' advisory course and their collaboration with management in policy formation remains vital to cyber security and reduction.

This is confirmed by the study of Salah 2022, it found the need to find measures that support the effectiveness of internal audits on cyber security based on the professional practices of internal audits, as these practices constitute a binding framework for the internal audit function.

The study (ISACA 2019, Bukht, et al2020, Kamiya,et,al, 2020, Berberoglu and Uzun, 2018) discussed the issue of cyber security and showed that cyber attacks are accelerating in a way that exceeds the development of security solutions, which led to these security attacks negatively affecting the Institutions and their clients from a financial point of view and affect the reputation of the institution.. In the same context, the study (Al-Zayoud 2021) concluded that there is an impact of internal audit represented by (efficiency, organizational status, and planning) in reducing cyber risks in Jordanian banks. It also concluded that there is no effect of internal audit neutrality in reducing cyber risks in Jordanian banks. While other studies discussed other topics that may affect cyber security, and in this context, the study (Al-Shaer and Al-Nasser 2019) concluded that there is an impact of cyber governance in reducing cyber threats in the Jordanian Zara Company (Holding).

Some studies have dealt with internal auditing and its role in information technology, including (Beerbaum ,2021, Acharya,2020 And Khersiat, 2020, Joshi, 2021, AL-Ramahi,2017) showed that the use of the lean methodology increases the efficiency and effectiveness of internal auditing and enhances added value, and that non-application negatively affects business performance, as it differs between business organizations according to size and culture.

iv. Study Problem:

In light of an environment dominated by the nature of digital technology and the increasing trend and acceleration towards technology and the use of advanced technology tools, and the accompanying huge revolution in storing data in digital format and on the Internet and cyberspace, and of course it was necessary for countries and institutions to find the necessary means and

procedures To protect this information, which is often information of a level of importance and sensitivity, in other words, a "secure digital infrastructure connected to cyberspace" must be found. In this environment, many questions arise that are looking for an answer, such as the relationship of internal audit departments with cyber security and the role of institutional culture in reducing its risks. Therefore, the researcher seeks in this study to answer a very important question, which is the impact of the internal flour departments combined in evaluating and managing cyber security risks and the mediating role of institutional culture in banks operating in Jordan.

v. **Study methodology**:

In order to reach the objectives of the study, the researcher relied the analytical approach descriptive to identify the impact of the internal audit department in evaluating and managing cyber security risks and the mediating role of institutional culture in banks operating in Jordan. Jordan as a tool for collecting data primary and information in preparation for benefiting from it.

1.1 Study hypotheses

The hypotheses were built as follows

H01: There is no significant effect statistically at a significant level ($\alpha \leq 0.05$) of the internal audit department combined (the application of an internal control system, the application of professional standards by internal audit departments, risk management methods and procedures, the role of audit committees) on the institutional culture in banks operating in Jordan .

H02: There is no significant effect statistically at the level of significance ($\alpha \leq 0.05$) for the internal audit department combined (the application of an internal control system, the application of internal audit departments to professional standards, risk management methods and procedures, the role of audit committees) on cyber security risk assessment and management.

HO3: There is no significant effect statistically at a significant level ($\alpha \leq 0.05$) of the internal audit department in evaluating cyber security risks and managing them in the presence of institutional culture in banks operating in Jordan.

1.1.1 Study population:

The population study consisted of the internal audit department, administrative managers, and employees of the Cyber Security Department in banks operating in Jordan. The number of questionnaires that were distributed reached 150, 120 of which were retrieved and analyzed (lHair,2007)The study consisted of a questionnaire divided into 3 sections, the first of which consists of 43 items related Measured by the internal audit department combined (the application of an internal control system, the application of professional standards by internal audit departments, methods and procedures for risk management, the role of audit committees, and its second section consists of 32 statements related to measuring the dependent variable, assessing and managing cyber security risks, and its third section consists of 13 statements And related to

the mediating variable is the institutional culture To measure the stability of the measurement tool, Cronbach's Alpha analysis was used (Ekolu and Quainoo,2019) To verify the stability of the measurement tool, where the percentage of the stability coefficient of the questionnaire as a unit was 80%, and these percentages exceeded the statistically acceptable percentage of 60%, which indicates the existence of correlation and consistency between the questionnaire statements

1.2.1 Analysis and Testing:

In this study, the descriptive analysis of the data was relied upon, based on the five-point Likert scale, and the hypotheses were tested on the Baron & Kenny test to test the mediating variable, the institutional culture. Description of the study sample answers

Through the standard deviations and arithmetic means, the answers of the study sample were described, which are related to internal audit management, cyber security and its management, and institutional culture.

Table (1)

standard deviation and arithmetic mean (applying a tight internal control system)

NO	Paragraph applying a tight internal control system)	Arithmetic mean	standard deviation
5	The internal auditor examines the procedures to ensure their compliance with laws, plans, systems and regulations, and how they contribute to activating the principles of governance.	4.2	0.42
3	There are procedures in the internal control system to ensure that the principles of corporate governance are applied	3.98	0.53

Source: Source: Prepared by the researcher

Table (1) shows that the highest arithmetic means, which is related to the application of a tight internal control system (returns to Paragraph No. (5), where it reached (4.20) and with a standard deviation (0.42), which is that the internal auditor examines the procedures to ensure their compliance with laws, plans, systems and regulations, and how they contribute to activating the principles of governance. The minimum arithmetic mean was 3.98) with a standard deviation of (0.53) due to paragraph (3) There are procedures in the internal control system to ensure that the principles of corporate governance are applied.
Table (2)

standard deviation and arithmetic mean (the application of professional standards by internal audit departments)

NO	Paragraph (internal audit departments applying professional standards)	Arithmetic mean	standard deviation
11	The internal auditor has independence from the activities he audits	4.23	0.48
7	The internal auditor submits a quarterly report to the Board of Directors and the Audit Committee on the extent of the company's commitment to the application of corporate governance principles and rules.	2.96	0.52

Source: Prepared by the researcher

Table (2) shows that the highest arithmetic mean for applying professional standards by internal audit departments goes back to paragraph (11). (0.52) refers to paragraph (7), where the internal auditor submits a quarterly report to the Board of Directors and the Audit Committee on the extent of the company's commitment to applying the principles and rules of corporate governance

Table (3)

standard deviation and arithmetic mean of risk management methods and procedures

NO	Paragraph (means and procedures for risk management)	Arithmetic mean	standard deviation
2	The Internal Audit Department sets systems for risk management procedures in the company to properly apply the principles of corporate governance	4.03	0.800
7	The internal audit activity plan is based on assessing the risks at least once a year. The internal audit activity monitors and evaluates the effectiveness of the risk management system in the Bank..	2.98	0.47

Source: Prepared by the researcher

Table (3) shows that the highest arithmetic mean of risk management methods and procedures belongs to paragraph (2), where it reached (4.03) with a standard deviation of (0.80). The internal audit department is developing systems for risk management procedures in the company to apply the principles of corporate governance in it properly, which is The minimum arithmetic mean was (2.98) with a standard deviation of (0.47) due to paragraph (7). The internal audit activity plan is based on assessing risks at least once a year. The internal audit activity monitors and evaluates the effectiveness of the risk management system in the bank.

Table (4)
standard deviation and arithmetic mean (the role of audit committees)

NO	Paragraph (role of audit committees)	Arithmetic mean	standard deviation
13	The Audit Committee takes the necessary measures to ensure that the company does not violate the laws and regulations in force in the country and the extent of its suitability for the principles of corporate governance.	4.11	0.41
5	The Audit Committee influences the achievement of objectives and the activation of the principles of corporate governance in the bank	2.8	0.40

Source: Prepared by the researcher

Table (4) shows that the highest arithmetic mean for the role of the audit committees in the bank goes back to paragraph (13), where it reached (4.11) with a standard deviation of (0.41). Its compatibility with the principles of corporate governance, while the minimum arithmetic mean was (2.8) with a standard deviation of (0.40) due to paragraph (5). The audit committee affects reaching the goals and activating the principles of corporate governance in the bank.

Table (5)
the standard deviation and arithmetic mean of institutional culture

NO	Paragraph (institutional culture)	Arithmetic mean	standard deviation

1	Initiate discussions about cyber security with the leadership team and communicate regularly with staff responsible for managing cyber risks	4.03	0.18
8	Innovation that includes security issues and planning is done from the start	3.89	0.88

Source: Prepared by the researcher

Table (5) shows that the highest arithmetic means belongs to paragraph (1), where it reached (4.03) and with a standard deviation of (0.18). Discussions about cyber security started with the leadership team and communicated regularly with the employees responsible for managing cyber risks. The lowest arithmetic mean reached (3.89) with a standard deviation of (0.88) due to paragraph (8), innovation is being promoted that includes security problems and planning from the beginning.

Table (6)
arithmetic mean and standard deviation for evaluating cyber security risks and managing them

NO	Paragraph (institutional culture)	Arithmetic mean	standard deviation
17	Develop a plan to continually reassess the cyber security maturity, risks, and objectives in your organization	4.28	0.47
6	Ensures that the Information Security Manager has a clear and direct line of communication to update you and the Board of Directors on threats in a timely manner	2.8	0.40

Source: Prepared by the researcher

Table (6) shows that the highest arithmetic means belongs to paragraph (17), where it reached (4.28) and with a standard deviation of (0.47). Develop a plan to continuously re-evaluate the maturity of cyber security and the risks and objectives related to it in your organization, as the lowest arithmetic mean reached (2.8) and with a standard deviation of (0.40). (Refers to paragraph (11) It is ensured that the Information Security Manager has a clear and direct line of

communication to inform you and the Board of Directors of threats in a timely manner Through the arithmetic means and standard deviations, the responses of the study sample related to the independent variable “internal audit management” were described, the mediating variable is the institutional culture, and the dependent variable is the assessment and management of cyber security risks, as in

Table No. (7)

Variable	Number	Mean	Stander deviation
Internal Audit Department	120	3.8138	.10760
Institutional culture	120	3.9760	.26790
Cybersecurity risk assessment and management	120	3.8609	.13535

Source: Prepared by the researcher

Through Table No. (7), it was found that the answers of the sample study were positive with regard to the internal audit department, as the total arithmetic mean was around the corresponding, reaching 3.8138), which means that there is a good level of internal audit management from the point of view of the internal auditors and the Cyber security Department , and administrative managers, as the total arithmetic mean was about corresponding to the institutional culture, reaching (3.9760), which means that there is a good level of institutional culture, and the answers were positive for the dependent variable, assessing cyber security risks and managing them, as the total arithmetic mean was about corresponding to (3.8609). Which means that there is a good level in evaluating cyber security risks and managing them. We find that the standard deviation of the variables Internal Audit Department (.10760) and institutional culture (.26790) Assessment of Cyber security Risks and Management (.13535) and the standard deviations were less than one correct for the variables This indicates that there is consistency in the opinions of the sample studied.

Table No. (8)
correlation between the variables of the study.

	Cybersecurity risk assessment and management	Institutional culture	Internal Audit Department

Cybersecurity risk assessment and management	1	.613	.203
Institutional culture		1	.248
Internal Audit Department			1

Source: Prepared by the researcher

The correlation between the variables is considered strong if the absolute value of the correlation coefficient is (=)or more than 50%. If the total value of the correlation coefficient is less than 50%. The correlation is considered weak, as the correlation coefficient between the dependent variable and the independent variable is positive, but it is less than 50%, as shown in Table No. (8). 0.203 the correlation coefficient between the dependent variable and the mediating variable is positive and strong because it is more than 50%, which is 0.613. The correlation coefficient between the independent variable internal audit management and the institutional culture variable appears positive as it reached (0.248). Table (9) shows the results of the simple regression analysis model of the effect of the internal audit department on the institutional culture. The results of the first equation according to the Baron and Kenny model (Zhao,2010)

Table (9)

R	.248[a]
R^2	. .062
F Value	7.764
F Significant	.006
Beta	.248
VIF	1.00
Standard Error	.222

Source: Prepared by the researcher

Table (9) shows that there is an impact of the internal audit department on the institutional culture, where the F value is (7.764), which is statistically significant, and the correlation between the internal audit department and the corporate culture is (0.248R), which indicates a statistically significant correlation. R2 indicates the effect of the internal audit department on Institutional

culture with a value of (.062), and that the coefficient of the independent variable is(B.248), while (0.222) = Standard error, which indicates the deviation of the data from its arithmetic mean, which is a very small percentage. Also, the value of the VIF of the model was (1.000) less than (10), which It indicates that there is no linear multiplicity problem between the variables, and that the value of sig = 000. Therefore, the (HO) is rejected and the (H1) is accepted, which states, "There is a statistically significant effect at the 0.05 significant level of the independent variable of the internal audit department on the mediating variable of institutional culture from the point of view of the study sample." Thus, the first condition was fulfilled according to the Baron & Kenny model, so Y = 1.617 + .619X, which represents the regression line equation

The second equation according to the Baron & Kenny model, which measures the impact of internal audit management as an independent variable on assessing and managing cyber security risks as a dependent variable without institutional culture as a mediating variable (total effect)(Zhao,2010)

Table(10)

R	.203[a]
R [2]	.041
F Value	5.072
F Significant	.03[b]
Beta	.203
VIF	*1.000*
Standard Error	.113

Source: Prepared by the researcher

Table (10) shows the effect of The impact of internal audit management on the assessing and managing cyber security risks where the value of F (5.072) it is statistically significant and the correlation between the independent variable and the dependent variable R (0.203), which indicates a statistically significant correlation and R2 indicates the impact of the Internal Audit Department on the assessment and management of cyber security risks with a value of (.041) and that the coefficient of the independent variable B (0.203) and the value of the VIF of the model was (1.000) Less than (10), which indicates that there is no problem of linear multiplicity between variables and that the regression coefficient of the independent variable Standard Error(0.113), which means the deviation of the data from its arithmetic mean, which is a very small percentage, and that the value of sig = .03b at the level of significance 5%, so the (HO)is rejected and accepts the (H1) that states "There is a statistically significant effect at a significant level of 0.05 for the

Internal Audit Department on the Cyber security risk assessment and management from the point of view of Study sample" This hypothesis shows the effect of Internal Audit Department on the Cyber security risk assessment and management, which is known as the total effect, and thus according to the Baron & Kenny model, the second condition has been achieved, and therefore Y=2.887+.255X represents the regression line counter.

The third equation in the Baron and Kenny model is the effect of the mediating variable on the dependent variable in the presence of the independent variable, which is the direct effect coefficient [30], which is the multiple regression equation Table No. (11) Shows the results of the multiple regression analysis model of the impact of the internal audit management on the assessment and management of cyber security risks with the mediating variable (institutional culture). Results of the third equation in the Baron and Kenny model

Table (11)

R	.615[a]
R^2	.378
F	35.564
Sig Med	0.00
Siq dep	.474
Siq total	0.00
Beta Internal Audit Department	.054
Beta Institutional culture	.599
VIF	1.066
Stander Error	
Internal Audit Department	.095
Institutional culture	.038

Source: Prepared by the researcher

We note from Table (11) the value of (F35.564), which shows that the effect of the internal audit management on the assessment and management of cyber security risks alarm is statistically

significant and that there is a correlation between the independent variable and the dependent variable with the presence of the intermediate variable (0.615R), which indicates a statistically significant correlation and R2 indicates the impact of the Internal Audit Department as an independent variable on the dependent variable Cyber security risk assessment and management and the mediating role of institutional culture with a value of .378)) and that the regression coefficient of the Internal Audit Department as an independent variable has reached (.054) The VIF value of the model was (1.066) less than (10) and this means that there is no linear multilinear problem between the study variables and that the value of sig = 000 Therefore, it rejects the (H0)and accepts the (H1) that states "There is a statistical significance at a significant level of 0.05 for the median variable. Institutional culture affects the dependent variable. Assessment and management of cyber security risks in the presence of the independent variable Internal Audit Management from the point of view of the sample study "Therefore, Y=2.398+.068X+.303X, which represents the regression line equation

The mediation of the institutional culture on the dependent variable is the evaluation of cybersecurity risks and their management is considered a total mediation, because when the mediating variable is present, the institutional culture becomes a total effect between the mediating variable and the dependent variable, because the value of siq is statistically significant = 0.00, while the independent variable does not predict the dependent variable in assessing security risks. Sperani and management mediated institutional culture because the siq value = .474

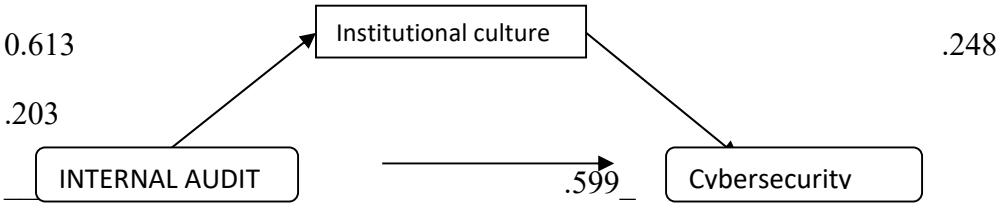

Figure (1)

Source: Prepared by the researcher

We consider mediation as total mediation when the direct impact, which is the impact of the internal audit department on the assessment and management of cyber security risks, which is (0.203) A closest to zero of the total impact, which is the impact of the internal audit department as non-independent on the dependent variable Cyber security risk assessment and management (0.599) and therefore the condition of total mediation has been achieved because the direct impact is closest to zero than the total impact

vi. Results and Recommendations

After analyzing the data and testing hypotheses according to the Baron & Kenny model, it was found that there is an effect of internal audit management on the intermediate variable (institutional culture) in the simple regression model, as the study showed that there is a significant statistically

impact of the internal audit department as a non-independent on the dependent variable Cyber security risk assessment and management, and this is confirmed by all previous studies, where the effect of the independent variable on the dependent variable according to the Baron & Kenny model(Zhao,2010) Direct impact The results showed that there is an effect of the institutional culture as an intermediate variable on the dependent variable Cyber security risk assessment and management, but the results showed that when mediating the institutional culture, the internal audit department does not predict in the assessment and management of cyber security risks, and this is considered according to the Baron & Kenny model[30] an indirect effect, and thus the study recommends that it requires internal audit departments To acquire the skills that enable them and help them to carry out internal audits in modern technology-based methods in order to develop a department capable of pace keeping with the developments dangerous in the digital environment, which is represented by the risks and threats contained in cyberspace, and the study also recommends the internal audit department to develop their skills related to modern technology and to be sufficiently aware of the risks related to it, and the study also recommends institutions to pay attention to their culture, which is the culture of cyber security that makes One of the objectives of the institution is to maintain the confidentiality and protection of information.

References:

Acharya, S. (2021). Agile Auditing for Increasing Efficiency. International Journal of Auditing and Accounting Studies, 3 (1), 79- 107

Alina ,Maria&Cerasela, SpÄƒtariu Elena ,Gabriela, Gheorghiu, 2017. "Internal Audit Role in Cybersecurity," Ovidius University Annals, Economic Sciences Series, Ovidius University of Constantza, Faculty of Economic Sciences, vol. 0(2), pages 510-513.

Amirhom,Jhan(2022) The Impact of the Internal audit quality in reducing cybersecurity risks and its repercussions on rationalizing investor decisions(Empirical study),Journal of financial and Business Research Vol,23-No,3

Al-Amarat, Faris Muhammad and Al-Hamamsah, Ibrahim 2022, Cybersecurity Concept and Challenges of the Age, 1st Edition, Amman: Dar Al-Khaleej for Publishing and Distribution.

Al-Bahi, Raghda, 2017, cyber deterrence, the concept, problems and requirements, Journal of Political Science and Law. Issue (1). Arab Democratic Center for Strategic, Political and Economic Studies, Berlin, Germany

Al-Fatlawi, Ahmed Abes Nehme 2016, Cyberattacks, their concept and the international responsibility arising from them in the light of contemporary international regulation, Al-Mohaqqiq Al-Hali Journal for Legal and Political Sciences, Issue (4) eighth year. Babylon University.

AL-Ramahi, N. (2017). Measuring the application of COSO framework for internal control from the point of view of the external auditors in the public shareholding companies listed on the Amman Stock Exchange. Zarqa Journal for Research and Studies in Humanities, 17(2), 471-482.

Al-Samhan, Mona Abdullah, 2020 Requirements for Achieving Cybersecurity for Administrative Information Systems at King Saud University, Journal of the College of Education, Issue 11, Mansoura University, Kingdom of Saudi Arabia, July.

Al-Shaer, Radwan Salem and Al-Nasser, Samira Khaled (2019), The Impact of Cyber Governance in Mitigating Cyber Threats in Jordanian Holding Companies: A Case Study of Zara Investment Holding Company, Jerash for Research and Studies (The System) Vol. 21, Special Issue, pp. 107-118.

Beerbaum, D. (2020). Application of Agile Audit: A Case Study Research. https://www.researchgate.net/publication/346652158_Application_of_agile_audit_A_case_study_research

Berberoğlu, Murat, Uzun, Uğur(2018)" the effects of cyber attacks on turkish banking sector, Economic and Management Issues in Retrospect and ProspectEdition: First Edition ,IJOPEC Publication Limited

Bukht,Tanvir,Roze,Muhammad,awan, Jawad,and Rizwan,ahmad(2020) analyzing cyber - attacks targeted on the banks of Pakistan and their solutions ,international journal of computer science and network security20(2)

Committee of sponsoring organizations of the treadway commission (COSO), (2019) ,Enterprise wide management (ERM) for Cybersecurity available athttp://www.coso.org/documents/COSO-Deloitte-Managing-Cyber-Risk-in-a-Digital-Age.pdf

Cybersecurity Handbook for Developing Countries, ITU 2014.

Dudin,Ahmed(2015)The Importance of Corporate Governance in Strengthening Control and Combating Corruption. "A Case Study on Jordan Petroleum Refinery Company"Zarqa Journal for Research and Studies in Humanities Volume 15, No 3,PP68-79

Ekolu, S. O. and H. Quainoo,(2019) ‘Reliability of assessments in engineering education using Cronbach’s alpha, KR and split-half methods’, Glob. J. Eng. Educ., vol. 21, no. 1, pp. 24–29, 2019

Hair, J. F.(2007) Research Methods for Business, vol. 49, no. 4. 2007. doi: 10.1108/et.2007.49.4.336.2.

He,Li Won Gyun,No and Tawe. Wang , (2018) ,SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors، International Journal of Accounting Information Systems, 30, Pp.40 – 55.

Institute of internal auditors (IIA), (2020) ,North american pulse of internal audit available at http://theiia.mkt5790.com/2020- pulse-of-internal-audit .

International Accreditation Forum (IAF), (2021) , Available at: https://iaf.nu/en/home/ .

ISACA, (2019),auditors have a role in cyber resilience ISACA Journal VOL 6 available at www.isaca.org

Islam M.S, Nusrat Farah, Thomas F. Stafford., (2018) ,Factors associated with security / cyber security audit by internal audit function an international study Managerial auditing journal , Pp. 377- 409, available at :10.1108/MAJ-07/2017-1595

Joshi, P. L. (2021). A Review of Agile Internal Auditing: Retrospective and Prospective. International Journal of Smart Business and Technology, 9(2), 13-32.

Journal OF banks, (2023) vol 42 no 2, https://www.ibookjo.com/books/AlBonok-Magazine-Issue2-42/18/

Kahyaoglu S.B and K. Caliyurt, (2018) ,Cyber security assurance process from the internal audit perspective managerial audit J. 33 (4) Pp. 360 – 376 available at http://doi.org/10.1108/MAJ-02-2018-1804

Kamiya, Shinichi, Koo, Kang Jun, Jungmin, Kim, Milidonis Andreas, Stulz, René M (2021) Risk management, firm reputation, and the impact of successful cyberattacks on target firms,Journal of Financial Economics, Volume 139, Issue 3, March 2021, Pages 719-749

KPMG (2020b). Internal Audit: Key Risks & Focus Areas 2021. https://assets.kpmg/content/dam/kpmg/ie/pdf/2020/12/ie-internal-audit-focusareas.pdf

Lois petros, George Drogalas, Alkiviadis Karagiorgos, Alkis Thrassou and Demetris Vrontis (2021) ,internal auditing and cyber security audit role and procedural contribution, international Journal of managerial and financial accounting, Vol. 13, No1 , Pp.25-47 ,available at : http://www.researchgate.net/publication/353255386 DOI 10.1504/IJMFA2021.116207

Othman, Mohamed Ahmed, (2022) Determinants of the effectiveness and function of internal auditing in cybersecurity risk management, the fifth scientific conference of the Accounting and Auditing Department, entitled Challenges and Prospects of the Accounting and Auditing Profession in the Twenty-First 30

Saleh, Nermin Mohamed Shaker 2022, Determinants of the effectiveness of the internal auditor for cybersecurity, the fifth scientific conference of the Accounting and Auditing Department, entitled Challenges and Prospects of the Accounting and Auditing Profession in the Twenty-First Century. Faculty of Commerce - University of Alexandria, pp. 1-24.

sergeja slapni car, Sergeja Slapničar, Marko Čular, Matej Drašček (2022) ,Effectiveness of cyber security audit, international Journal of accounting information systems, Pp.1-21, available at : http://doi.org/10.1016/j.accinf.2021.100548.

Shahimi S. and N. Mahzan, (2018), Building a research model and hypotheses development and findings of Explorator Interviews, International Journal of Management Excellence

Shamsuddin , amanuddinn, (2018) ",the effectiveness of internal audit functions in managing cybersecurity in malaysia's Banking institutions" international Journal of industrial management IJIM ISSN print 2289 – 9286 Volume 4, Pp. 61- 69

Slapnicar, S., Vuko, T., Cular, M., and Drascek, M. (2022). Effectiveness of cybersecurity audit. International Journal of Accounting Information Systems, 44,

Vuko Tina, Sergeja Slapničar, Marko Čular, Matej Drašček, (2021) ,key drivers of cyber security audit effectiveness the neo-institutional perspective, Pp.1-43 available at http://ssrn.com/abstract=3932177 .

Zhao X., Lynch, J. G. and Chen, Q. (2010)'Reconsidering Baron and Kenny: Myths and truths about mediation analysis', J. Consum. Res., vol. 37, no. 2, pp. 197–206, , doi: 10.1086/651257.