The Relationship between Network Security Policies and Audit Evidence Documentation: The Accounting Information Security Culture as a Mediator

Mohammad Naser Musa Hamdan[1]

[1] Accounting Department, Al al-Bayt University, Jordan

Correspondence: Mohammad Naser Musa Hamdan, Accounting Department, Al al-Bayt University, Jordan. E-mail: mohd_naser78@yahoo.com

Received: October 12, 2017 Accepted: October 28, 2017 Online Published: November 20, 2017

doi:10.5539/ijbm.v12n12p168 URL: https://doi.org/10.5539/ijbm.v12n12p168

Abstract

The purpose of this study is to explore the relationship between network security policies (the department policy, system director policy, user policy, information security officer policy) on the one hand, and audit evidence documenting on the other hand. As the security, culture of accounting information has been introduced as a variable mediating that relationship. The researcher sent (450) questionnaires to all the companies listed on the Amman Stock Exchange in Jordan equivalent to (228) company until 2015. The study found that there is a significant relationship between networks (the department policy, system director policy, user policy, information security officer policy) and documentation of the audit evidence. While the respondents said that, there is not a significant relationship between information security officer and policy and documentation of the audit evidence. Besides, the value of the correlation coefficient between network security policies and documentation of audit evidence had increased from (0.56) to (0.62), after entering the variable of security culture of accounting information systems to demonstrate its impact as a variable rate of the regression model and this result demonstrates the importance of awareness of security culture of the companies. These results will be very useful for those are interested, especially auditors to help them to appreciate the importance of documenting the audit evidence of network security and their implementation on the ground.

Keywords: network security policies, audit evidence documentation and accounting information security culture

1. Introduction

The mass development of the information revolution on the one hand and the communications revolution on the other hand led to a significant progress in the electronic operation of accounting data with business organizations (Buccioli et al., 2015; Saleh, 2014). Which mirrored its effect on the methods and procedures of audit, although the audit objects in general are considered as one regardless the operating quality of manual or electronic data, but the audit procedures used by the auditor in conducting the tests may have been changed in response to the changing nature of each of the inputs elements and data operating processes and the nature of the output elements (Arens et al., 2012; Simkin et al., 2014). From here, governments in most countries are permanently seeking to develop rules and foundations and principles describe the mechanisms of correct and safe dealing of information, in particular those flows through the network in order to maintain this information from loss and damage, especially to deal (Abdullah & Fares, 2016), in both the public sector or private sector, especially in accounting information for its importance and its disclosure, and defining the roles (Yoon & Zhang, 2015) and duties that must be performed by the staff in order to achieve an appropriate level of security and protection for this information, and make them available when if needed for people and entities who have access authorization (Cavelty & Mauer 2016, NIACSS, 2012). The information flow across networks makes it difficult to follow up and verify that information (Romney et al., 2013), and in particular as long the complexity of networks is increased of and consequently such shall generates difficulties to find appropriate audit evidence (Simkin et al., 2014). Hence auditor would need to study and understand the types of electronic accounting information systems (WGITA - IDI., 2014), and its impact of the regulatory aspect over the company, and on the extent of data and information clarity inside electronic accounting information (Mousa & Al Qa'qa'a, 2016), and the existence of relative important distortions (Abdullah & Fares, 2016), and thereby the ability of the auditor to realize the objectives of auditing process shall be increased in the light of these variables based on all the afore contained by the study to detect the relationship between networks security policies and their impact on documenting audit evidence in light of security culture enjoyed by business organizations these days.

1.1 The Problem of the Study

When determining the sufficiency and appropriateness of evidence of electronic proof that were collected in order to assist the auditor to express an audit opinion on the financial statements, the auditor must take into account the risks associated with the use of this type of evidence(Tan, 1995), where you cannot determine the extent of appropriate sufficiently through the examination of the electronic proof of evidence (Mousa & Al Qa'qa'a, 2016; Backof, 2015) as is in the case in the hard copy proof as printing the electronic information outputs or reading them on the screen is only one model and cannot give an indication of the origin of the information or its validity also it cannot confirm the completeness or comprehensiveness of the information (Abdullah & Fares, 2016) and thus the auditor should ensure that the control and techniques systems relating to the establishment, processing , transmission and maintaining the electronic information sufficient systems so that it can ensure the credibility of the information (Arens et al., 2012). It may consequent in the electronic operating environment the appearance of several problems, including the problem of the disappearance of the set of books and documents where it became having a new model thus several stages were incorporated to be shown as one stage in the electronic operating also the impact of data electronic operating extended to the place of operation (Hamed, H., & Al-Shaer, E. 2006) where these operations became fully carried out within the accountant itself and it shall consequent thereof the proof guide become invisible in its nature in contrary to what the auditor accustomed under the manual systems (Romney et al., 2013). The proof of evidence in light of data electronic operating in programs, records, operating systems, followed configuration system and engineering design of PCs, software and the proof of evidence shall lose its strength if it exposed to any of the errors that can occur in the value of the primary elements when introduced into the computer, when updated, when stored or when you make some modifications therein (Arens et al., 2012). The tremendous developments did not stop at the use of information systems and computer technologies in information collection, processing, transmitting, maintaining presenting, and adapting the references to this environment (WGITA - IDI., 2014), as the approach of information technology with the information systems integration led to the flow of information without the need for line of communication (Abdullah & Fares, 2016). The integrated information systems environment is deemed a paperless environment where information is exchanged without restrictions and obstructions of place, as they are submitted from one application to another and from one facility to another or from one country to another through electronic networks (Mousa et al., 2016) In this context, the auditor is obliged to the collect the electronic information as proof of evidence of auditing (Arens et al., 2012).

2. Literature Review

2.1 Networks Security Policies

In the age of digital information, the free movement of information, and the credence of individuals, institutions and governments on information and communication technology, in addition to the availability of the technology easily the spread of open-source software, information `obtrusiveness of sites (NISTC, 2008), and the spread of programs and applications in an unprecedented way and cheaply; especially pirated programs or those distributed by sites of pirates, networking between systems, and the emergence of multimedia and its extensive use, together with the similarities between them, especially at the level of methodologies and techniques in programming, we find ourselves face an urgent need to have security policies for the networks that information are transmitted through it. Therefore, that security is an essential condition of trust realization. The purpose of the network security policies is to clarify the mechanism of dealing with informatics network elements securely, and identifies things required to be available to ensure the security and protection of systems connected to these networks from the dangers and threats (NISTC, 2012), in order to reach a stabled and secured network able to meet the requirements of business of the related business organizations (Romney et al., 2013). In addition, network security policies are essential lines demonstrate frameworks, define roles and responsibilities and show best practices and minimum commitment required to be taken into account and the work done by various employees and dealers with those networks. This policy covers all the elements and components of information and resources on its local network and the network and wide-ranging, both wired and wireless (NISTC, 2008), which model the communications infrastructure to provide various communication techniques for users.

2.2 Documentation of Audit Evidence

The purpose of the information security audit policy is to ensure the safety, security, availability of information and resources, and the disclosure of the possibility of the occurrence of security incidents (WGITA - IDI. 2014,Okab, R. 2013), and to ensure the existence and effectiveness of the procedures used in the business organizations and their compatibility with the information security and protection, risk assessment (Arens et al., 2012, Hai, P. T., 2016), and on the other hand, the support of measures that help to identify weak points. Audit policies of information security cover all informational resources, records and information resources, procedures, instructions, powers and responsibilities and any acts linked to any other internal documents or external audit policy (WGITA - IDI., 2014). The documentation accounting information processes audit operations are only a record of audit works that have been done, or an audit evidences that support the audit findings and conclusions, in addition, the information auditor must ensure the save of audit results and audit evidences in a manner consistent with the reliability, completeness, adequacy, validity and risk avoidance requirements (Arens et al., 2012,Alqadi, F. S., 2017). As for its importance, the information security auditor must confirm on saving the audit process to ensure that the subsequent verification of audit procedures and all should include the appropriate ways of documentation (WGITA - IDI. 2014, Peltier, T. R. 2016).

2.3 Accounting Information Security Culture

The accounting information security culture in the light of these technological developments is not easy and the term information security is a comprehensive concept containing network security, the used devices security, the organizational security and legal security(Boss, S., Kirsch, L., Angermeier, I., Shingler, R., & Boss, R. 2009). To develop a comprehensive vision for the information protection and security, we must take into account the security policy, devices and tools security, networks security, organized security and legal security. As security policy is considered as the security cover of all aspects of security, which provides how to accomplish security and it should be built on the requirements and not on technical considerations(Whitman, M., &Mattord, H. 2011).In addition, political goals of any security policy must be to keep the confidentiality, integrity, perfectness and availability of all the informational wealth assets of companies and their communications. Confidentiality refers to confidential information, which is not viewed only by some people, such as managers, supervisors and some users. This information of the company and some users must be kept within the company and it maintains the information from being viewed by unauthorized or sudden disclosure. Safety and perfection refer to the information and data of the company. It must be as accurate and very modern. Integration or safety protects the information from unauthorized or sudden modification. Finally Availability refers to access to information and sources of the company, it is very important that information and company sources are easily available. Availability ensures a reliable data access whenever and wherever the need arises. The security policy must take into account these three objectives when studying any potential threats on the company. Once the development and approval of security policy(Peltier, T. R. 2016), it must be placed in the space of experiment and application. In addition, it is necessary to review the security policy on a regular basis to reflect the evolution and change of the company. The security program will be successful if the audit of dangers continued periodically with the administrative and legal approvals, which lead to audit the political procedures and daily responsibilities in a manner that shall ensure the documentation of all the audit evidence.

2.4 The Relationship between Network Security Policies, Documentation of Audit Evidence and Accounting Information Security Culture

It is important that the dealers of information to realize the extent of their importance and sensitivity, through consolidation of the security culture, in another word, focusing on security either at the stage of building information networks, or in the stage of development (Ghernaouti-Hélie, S., 2007), and dissemination of awareness methods and guidance in thinking and behavior in the use of information networks. On the other hand, all business organizations today are increasingly dependent on information networks, and herein lies the need to trust the information (Romney et al. 2013, Damenu, T. K., & Beaumont, C. 2017), and the only way to provide security effectively is an adoption of the approach that takes into account the good interests of all beneficiaries of this information (Ghernaouti- Hélie, S., 2007). The accounting information is the most sensitive information for its association to financial matters. Here we have to encourage a culture of security as a mean to protect accounting information (Selamat, M. H., & Babatunde, D. A. 2014). In addition, documentation of awareness about the risks of information networks (Mousa & Al Qa'qa'a, 2016), including public policy practices, measures and procedures available to address these risks, and the need to be followed and implemented (Abdullah & Fares, 2016). Also, business organizations need to build more trust among all users of information networks as they should be aware of the information networks security and to promote it in themselves, and how to behave at the proper time and cooperatively. Users must do risk assessment and design appropriate security, its implementation and adoption of a comprehensive approach towards the security department (Ghernaouti-Hélie, S., 2007).

2.5 Hypotheses of Study

Pursuant to the problem of the study and the literatures above, the hypotheses can be formed as follows:

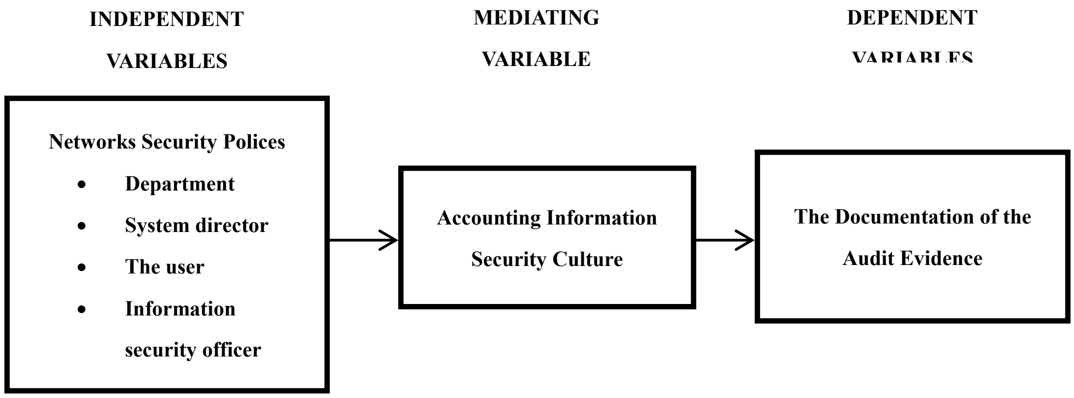

Figure 1. Schematic diagram of the research model

H_1: There is an important relationship between networks security polices and documentation of audit evidence.

H_{1a}: there is an important relationship between the department policy and documentation of audit evidence

H_{1b}: There is an important relationship between the system director Policy and documentation audit evidence.

H_{1c}: There is an important relationship between the user policy and documentation of the audit evidence.

H_{1d}: There is an important relationship between information security officer policy and documentation audit evidence.

H_2: There is a positive relationship between the documentation of the audit evidence and the accounting information security culture policies.

H_3: The accounting information security culture mediates the relationship between network security and documentation of the audit evidence policies.

H_{3a}: the accounting information systems security culture mediates the relationship between the department policy and the documentation of the audit evidence.

H_{3b}: the accounting information systems security culture mediates the relationship between the system director policy and documentation audit evidence.

H_{3c}: the accounting information security culture mediates the relationship between the user policy and documentation audit evidence.

H_{3d}: the accounting information security culture mediates the relationship between the information security officer and documentation audit evidence.

3. The Study Methodology

3.1 The Study Society and Its Samples

The study society consists of all listed companies in the Amman Stock Exchange equivalent to (228) up to 2015 (http://www.ase.com.jo/en).

About (150) companies were randomly selected from the list and this sample size was deemed appropriate (Roscoe, 1975, as cited in Saharan (2000)). Questionnaires were sent to (450) respondents and (112) responses were received, a response rate of (24.9%). Most of the respondents are either the head of the finance department (43respondents or 38.4%), the head of the audit department (39respondents or 34.8%) and the head of IT department (30respondents or 26.8% percent).

3.2 Instruments of Studies

To achieve the objectives of the study we prepared and developed a questionnaire by taking too into account the previous literatures and previous studies related to the subject of study and consulted a number of specialists and experts in this field. The questionnaire consisted of two main parts: the first part consists of general information included clauses relating to personal variables of members of the society, namely, (job title). The second part consists of (4) areas related to the independent variable network security policies, namely, (the department policy, system director policy, information security officer policy, and user policy). NISTC (2012) was sourced to formulate paragraphs of this magazine (see tables nos (2-6)) and a single axis related to the dependent variable of documentation of the audit evidence. WGITA - IDI (2014) was sourced to formulate paragraphs of this area (see Table 7). As well as one axis of the mediator of accounting systems information security. Ghernaouti-Hélie, S. (2007) was sourced to formulate paragraphs of this area (see Table 8).

3.3 Reliability of Instruments and Reliability of Application

To ensure the reliability of study's instrument, the reliability of application has been verified through the distribution of the study's instrument on an exploratory sample of (20) persons from outside the study sample twice with a time-lag of (two weeks) and extracted the Pearson correlation coefficient (Pearson Correlation) from their marks twice, as is shown in table (1), which shows the reliability coefficients and Pearson correlation coefficient of the dimensions of the study and the instruments as a whole. As it is shown from the table that the reliability of the dimensions of the study coefficients are ranged between (0.75-0.86), all are high and acceptable values for the purposes of the application as well.

Table 1. Reliability coefficients of (Cronbach's Alpha) and Pearson correlation coefficient of the study instrument

Field	Dimension	Reliability coefficients of (Cronbach's Alpha)	Stability reliability coefficients of (Pearsoncorrelation)
Field of information security policy	Department policy	**0.77**	**0.86**
	System director policy	**0.83**	**0.84**
	Information security officer policy	**0.75**	**0.76**
	User policy	**0.82**	**0.87**
	Field of information security policy as a whole	**0.79**	**0.85**
Documentation of audit evidences		**0.86**	**0.83**
Security culture		**0.77**	**0.81**
Instrument as a whole		**0.83**	**0.81**

3.4 Amendment of Scale

To analyze the data and test hypotheses have been relied on the Likert scale Quintet in answering paragraphs, according to the following score: score (1) reflects approval in a very low- degree, degree (2) reflects approval a low-score, score (3) reflects approval moderately, degree (4) reflects approval in a high- degree, degree (5) reflects approval in a very-high degree, in order to interpret the arithmetic means of estimations by the study sample individuals on each paragraph of the questionnaire, but with respect to the limits adopted by this study, when commenting on the arithmetic mean of the variables contained in the study sample it is and to determine the degree of approval , as the researcher has identified three levels; namely (high, medium, low) based on the following equation:

- Length of interval= (upper limit of substitution - lower limit of substitution)/ number of levels (5-1)/3= 4/3= 1.33, thus the levels shall be as follows:
- Low approval score from 1-2.33
- Medium approval scores from 2.34- 3.67
- High degree of approval from 3.68- 5

Analysis and discussion of hypotheses

In this part, we will present the results of the study, which aimed to identify the relationship between network security policies and documentation of audit evidence: the accounting information systems security culture, so by testing its hypotheses, as follows:

3.5 Results Related to Arithmetic and Standard Deviations Averages to the Field of Network Security Policy Dimensions

The arithmetic and standard deviations averages of the approval of individual respondents on the dimensions of the network security policy field were extracted therefrom, where the results were as shown in Table 2.

Table 2. The arithmetic and standard deviations averages of the approval of individual respondents on the network security policies field dimensions in descending order

Rank	Number	Dimension	Arithmetic average	Standard deviation	Assessment degree
1	4	User policy	4.30	0.59	High
2	3	Information security officer policy	4.24	0.56	High
3	1	Department policy	3.93	0.42	High
4	2	System director policy	3.06	0.35	Medium
Field of information security policy					High

Table 2 shows that the arithmetic averages of the answers of the samples individual respondents from the field of network security policies dimensions are ranged between (3.06-4.30), as the dimension of "User Policy" came in first place the with an average of (4.30) assessment score of high, the dimension of "information security officer policy" in the second place came with an average of (4.24) assessment score of high, the dimension of " department policy" came in third place after with an average of (3.93)) assessment score of high, the dimension of "system director policy" came in fourth place and the last with an average of (3.06) assessment score of, and arithmetic average of network security policies field (3.68) assessment score of high.

As well arithmetic averages and standard deviations were extracted of the answers of sample individuals respondents study of paragraphs of each dimension of the security policy field dimensions of the networks separately, tables (3-6) illustrate thereof.

Table 3. The arithmetic and standard deviations averages of the approval of individual respondents on the dimension of "Department policy" in descending order

Rank	No.	Paragraph	Arithmetic average	Standard deviation	Assessment degree
1	3	Full documentation of the informational networks of the department includes clear and understandable network graphics determining the its elements and determine the way to be linked to each other	4.43	0.64	high
2	1	Appropriate instructions for dealing with the informational network elements of the department shall be developed	4.41	0.68	high
3	2	Appropriate powers of the specialists of operation, maintenance and sustaining the networks functions shall be developed based on the functional description of each of them	4.39	0.70	high
4	5	Passwords for network access shall be set out and shall e given to the authorized individuals in conformity with the passwords policy	4.09	0.87	high
5	6	All elements of the system shall be audited	4.08	0.92	high
6	4	The configurations of the network devices shall be saved in secured place	4.07	0.88	high
7	7	The minimum of broadband network speed shall be provided	3.19	0.95	Medium
8	8	The commitment of users and employees shall be monitored to the national policies of safety and security of information	2.79	0.63	Medium
Dimension of department policy as a whole			3.93	0.42	high

Table 3 shows the arithmetic average of the approvals of the sample individuals respondents on the dimension of "Department policy" range from (2.79-4.43) the upper was the paragraph no. (3) stipulates:" Full documentation of the informational networks of the department includes clear and understandable network graphics determining it’s elements and determine the way to be linked to each other" and the lower was paragraph was the paragraph no. (8) stipulates that: "The commitment of users and employees shall be monitored to the national policies of safety and security of information". The overall general average of the dimension was equal to 3.93with high score assessment.

Table 4. The arithmetic and standard deviations averages of the approval of individual respondents on the dimension of "system director policy" in descending order

Rank	No.	Paragraph	Arithmetic average	Standard deviation	Assessment degree
1	7	facilitating the audit process on the systems, database, operating systems, employees and users devices in consistency of the information security audit policy	3.64	1.06	Medium
2	1	Consistency of specifications related to devices shall be confirmed, as well applications of informational networks in the department with the national policies of safety and security of information.	3.44	0.91	Medium
3	2	Providing lists of with the numbers of computers and servers to following up their numbers and the problems that may occur upon to guarantee the best execution	3.24	0.92	Medium
4	3	Installing, controlling, following up system operation of information network of the department	2.90	0.68	Medium
5	4	Controlling the devices able to connect and access to the different devices of the department by the access control lists.	2.83	0.60	Medium
6	5	Controlling the networks and the system of their management performance at once and submit reports thereof to the senior management in the department to approve them based on the movement records of information flow through networks	2.73	0.57	Medium
7	6	Following up whatever shall be updated of information about the existence of any gaps within operation systems of the devices of management of information network of the department	2.63	0.57	Medium
Dimension of system director policy as a whole			3.06	0.35	Medium

Table 4 shows the arithmetic average of the approvals of the sample individual is respondents on the dimension of "system director policy" are ranged from (2.63-3-64) the upper was the paragraph no. (7) stipulates:"facilitating the audit process on the systems, database, operating systems, employees and users devices in the consistency of the information security audit policy" and the lower was paragraph was the paragraph no.(6) stipulates that:" Following up whatever shall be updated of information about the existence of any gaps within operation systems of the devices of management of the information network of the department" overall general average of the dimension was equal to 3.06with high score assessment.

Table 5. The arithmetic and standard deviations averages of the approval of individual respondents on the dimension of "information security officer policy" in descending order

Rank	No.	Paragraph	Arithmetic average	Standard deviation	Assessment degree
1	1	Audit and revision processes shall be carried out by the approval of senior management in the department to assess the extent of the consistency the aspects of informational security in the net works.	4.29	0.61	High
2	2	It shall following up the reports of the security problems faced or are facing by the informational networks in the department and assist in solving them	4.19	0.70	High
Dimension of information security officer policy as a whole			4.24	0.56	High

Table 5 shows the arithmetic average of the approvals of the sample individual is respondents on the dimension of "information security officer policy" are ranged from (4.19-4.29) the upper was the paragraph no. (1) stipulates: "Audit and revision processes shall be carried out with the approval of senior management in the department to assess the extent of the consistency the aspects of information security in the networks." and the lower was paragraph was the paragraph no.(2) stipulates that: "It shall follow up the reports of the security problems faced or are facing by the informational networks in the department and assist in solving them" and the overall general average of the dimension was equal to 4.24 with high score assessment.

Table 6. The arithmetic and standard deviations averages of the approval of individual respondents on the dimension of "user policy" in descending order

Rank	No.	Paragraph	Arithmetic average	Standard deviation	Assessment degree
1	2	Saving the files and information on the devices determined by the system manager as file servers	4.38	0.72	High
2	1	Non-changing, solving or connecting any device to the department's informational networks without obtaining a prior written consent by the senior management in the department according to the policy of controlling the change and desktop policy as well the laptops policy	4.22	0.73	High
Dimension of user policy as a whole			4.30	0.59	High

Table 6 shows the arithmetic average of the approvals of the sample individuals respondents on the dimension of "information user policy" range from (4.22-4.38) the upper was the paragraph no. (2) stipulates: "Saving the files and information on the devices determined by the system manager as file servers" and the lower was paragraph was the paragraph no.(1) stipulates that:" Non-changing, solving or connecting any device to the department's informational networks without obtaining a prior written consent by the senior management of the department, according to the policy of controlling the change and desktop policy as well the laptops policy" and the overall general average of the dimension was equal to 4.30 with high score assessment

3.6 Results Related to Arithmetic Averages, Standard Deviations of Documentation Audit Evidence

The arithmetic and standard deviations averages of the approval of individual respondents on the dimensions of the documentation audit evidence field was extracted there from, where the results were as shown in Table 7.

Table 7. The arithmetic and standard deviations averages of the approval of individual respondents on the dimension of "documentation audit evidence " in descending order

Rank	No.	Paragraph	Arithmetic average	Standard deviation	Assessment degree
1	1	Planning and preparing for audit field and objectives	4.13	0.89	High
2	6	Results, conclusions and recommendations	3.89	0.89	High
3	4	Accomplished Steps of audit	3.79	0.86	High
4	3	Developing audit program	3.77	0.84	High
5	5	Evidences collected during auditing	3.76	0.89	High
6	2	Developing a general and detailed description of audit field	3.75	0.97	High
Dimension of documentation audit evidence policy as a whole			3.85	0.56	High

Table 7 shows the arithmetic average of the approvals of the sample individual is respondents on the dimension of documentation audit evidence policy “range from (4.22-4.38) the upper was the paragraph no. (1) stipulates: "Planning and preparing for audit field and objectives" and the lower was paragraph was the paragraph no. (2) stipulates that:" Developing a general and detailed description of audit field" and the overall general average of the dimension was equal to 3.85 with high score assessment

3.7 Results Related to Arithmetic Averages, Standard Deviations of Accounting Information Security Culture

The arithmetic and standard deviations averages of the approval of individual respondents on paragraphs of accounting information security culture field was extracted there from, where the results were as shown in Table 8.

Table 8. The arithmetic and standard deviations averages of the approval of individual respondents on the dimension of "accounting information security culture policy" in descending order

Rank	No.	Paragraph	Arithmetic average	Standard deviation	Assessment degree
1	3	(Department director, user, information security office) shall respect the legal interests of accounting information systems	4.85	0.36	High
2	2	(Department director, user, information security office) are responsible of accounting information system and information networks security	4.77	0.48	High
3	1	(Department director, user, information security office) must be aware with the need of accounting information system and information networks security	4.76	0.49	High
4	4	Accounting information system and information networks security must be in consistency with community values.	4.12	0.49	High
5	6	(Department director, user, information security office) must enroll security as a basic element in accounting information systems and their networks	3.97	0.87	High
6	5	(Department director, user, information security office) must assess risks	3.96	0.96	High
7	7	(Department director, user, information security office) must adopt a comprehensive towards the security management	4.12	0.94	High
Dimension of accounting information security culture policy as a whole			4.46	0.66	High

Table 8 shows the arithmetic average of the approvals of the sample individuals respondents on the dimension of "accounting information security culture policy" range from (3.96- 4.85) the upper was the paragraph no. (3) stipulates:"Department director, user, information security office shall respect the legal interests of accounting information systems" and the lower was paragraph was the paragraph no. (7) stipulates that:" Department director, user, information security office must adopt a comprehensive towards the security management" and the overall general average of the dimension was equal to 4.46 with high score assessment

4. Hypotheses Test

To validate the $\mathbf{H_1}$ and whatever ramified there from ($\mathbf{H_{1a}}$, $\mathbf{H_{1b}}$, $\mathbf{H_{1c}}$, $\mathbf{H_{1d}}$), was applied multiple regression equation to study the relationship between network security policies and documentation of audit evidence as a whole, Table 9 shows.

Table 9. Results of application multiple regression equation to study the relationship between network security policies and documentation of audit evidence

Dimension	ß	T	Sig	R	R²	F	Sig
Department policy	0.42	7.08	0.00				
System director policy	0.44	6.84	0.00				
User policy	0.13	2.04	0.04	0.86	0.74	74.45	0.00
Information security officer policy	0.04	0.70	0.49				

The previous results Show as follows:

Results of $\mathbf{H_1}$: an existence of a relationship between network security policies and documentation of audit evidence, as the value of the complex correlation coefficient (R) is equal to (0.86) which is the value of significant level and indicate the degree of correlation coefficient significantly between the independent variables and dependant variable value (R-square) was equal to (0.74), it is a significant value that interprets there is a relationship between the network security policies and documentation of audit evidence interprets that networks security policies s that the value of (86%) of the change in the documentation of audit evidence as a whole, and the test value (F) reached (74.45) in sig. (0.00), it is a significant level value indicative of a variation in the ability of the independent variables on influencing the dependent variable, and therefore we accept the hypothesis $\mathbf{H_1}$.

H_{1a}: the existence of an important significance level relationship between the department's policy and documenting of audit evidence, as values (ß, T) reached (0.42, 7.08) they are significant level values and therefore we accept the hypothesis H_{1a}.

H_{1b}: the existence of an important significance level relationship between the system director policy and documenting of audit evidence, as values (ß, T) reached (0.44, 6.84) they are significant level values and therefore we accept the hypothesis **H1b**.

H_{1c}: the existence of an important significance level relationship between the user policy and documenting of audit evidence, as values (ß, T) reached (0.13 2.04) they are significant level values and therefore we accept the hypothesis **H1c.**

H_{1d}: the existence of non- significant level relationship between the information security policy and documenting of audit evidence, as values (ß, T) reached (0.04, 0.70) they are non-significant level values and therefore we reject the hypothesis *H1b* in its proven model and we shall accept **H01b**.

H_2: **There is a positive relationship between the documentation of the audit evidence and accounting information systems security culture policies**.

To validate this hypothesis we used simple regression test, which the results showed in the table (10) and there is a medium direct relation between documentation of audit evidence and accounting information systems security culture policies, as the value of this relationship reached (0.29), and through value the coefficient of determination (R square) it is shown that the documentation audit evidence audit policies level interprets that rate (8%) of the variance in the variable of accounting information systems culture security, and because the value (F) is equal to (10.04), and its significance level was (0.00), accept the hypothesis $\mathbf{H_2}$.

Table 10. Results of simple regression test between documentation of audit evidence and accounting information systems security culture policies

Hypothesis	R	R²	DF	F	Sig
is a medium direct relation between documentation of audit evidence and accounting information systems security culture policies	0.29	0.08	111	10.04	0.00

To validate the $\mathbf{H_3}$ and whatever ramified there from ($\mathbf{H_{3a}}$, $\mathbf{H_{3b}}$, $\mathbf{H_{3c}}$, $\mathbf{H_{3d}}$), was applied hierarchical multiple regression test which its result is shown in Table 11.

Table 11. Results of hierarchical multiple regression test of the impact of accounting information systems security culture on the relationship between networks security and documentation of audit evidence policies

Step	Dependent variable	(β)	T Value	Sig	(R)	(R²)	(R²) change	Value F	Value F Change	Sig
First step	Department policy	0.43	7.08	0.00						
	System director policy	0.44	6.84	0.00						
	User policy	0.13	2.05	0.04	0.56	0.31	0.29	12.93	12.93	0.00
	Information security officer policy	0.04	0.70	0.49						
Second step	Department policy	0.43	7.19	0.00						
	System director policy	0.46	7.04	0.00	0.62	0.39	0.36	14.88	17.18	0.00
	User policy	0.15	2.25	0.03						
	Information security officer policy	0.06	0.91	0.37						
	accounting information systems security culture policy	0.08	1.52	0.13						

4.1 Dependent Variable: Documentation of Audit Evidence

The value of the correlation coefficient between network security and documentation of audit evidence policies increased from (0.56) to (0.62), after entering variable of accounting information systems security culture to demonstrate its impact as an amended variable regression form, Table (11) shows also the value of the coefficient of determination (R-square) of network security the policies has reached (0.31), and that the change in the coefficient of determination (Change2 R / R-square change) accounting information systems security culture has reached (0.39), and value (F change) has reached (12.93) at the trust level (0.000), which confirms the significance of regression at the trust level is (α ≤ 0.05), which means that the accounting information systems security culture has contributed to improve the impact of network security policies on documentation of audit evidence, where from explanation it added the amount of (0.06) of the variance in the documentation of audit evidence to increase the total value of this interpretation to (17.15). Table (11) as well shows the value of (F) for the first model has reached (12.93) at the trust level (Sig = 0.000), which confirms a significance of regression at the level (α ≤ 0.05), and when the four degrees of freedom (df = 4), as well table (11) shows that the value of (F) of the second model has reached (14.88) at the trust level (Sig = 0.000), which also emphasizes the significance of regression at the level (α ≤ 0.05), and when also degrees of freedom (df = 5), and thus accept the **H3** and whatever are ramified there from of sub- hypotheses.

5. Conclusion

Security policy networks aim to illustrate how to deal with the information network elements securely, and identify the things required being available in these components to ensure the security and protection of connected systems on these networks, in order to reach a stabled and secured network able to meet the requirements of business of the related business organizations. This policy covers all the elements and components of information and resources connected to its work in the network, which form the communications infrastructure to provide various communication techniques for users. There is a close correlation between the audit evidence and information security policies and in particular the accounting ones, those policies mainly provide some kind of proof evidence in the audit, which helps the companies or individuals in building fundamentals of security and determining the general framework of the duties of staff, consultants and those concerned with accounting information management and their applications. In addition, network security policies are considered the primary concern sought by companies, as they seek to benefit from the accreditation of information and communication technology to support the credibility of the data and protect it from tampering, vandalism and the precision of control. As maintaining the confidentiality and security of information is a top priority in companies as they constantly seek to take the appropriate measures to protect the confidentiality of information and prevent them from unauthorized access, since the protection of information systems in particular accounting information systems (for its relative importance) is the responsibility of every employee, and herein comes the role of the company policy in dissemination of the culture of security systems to observe the working together consciously by the staff.

In this study, which aimed to explore the relationship between network security policies, on the one hand and documentation of audit evidence on the other hand. As the accounting, information security culture has been introduced as a variable mediating that relationship. The study found a relationship between network security policies and documentation of the audit evidence as the value of the complex correlation coefficient (R) was (0.86), and by the value of the coefficient of determination (R square) it shows that the dimensions of the networks security policies interpret the value of (74%) of the change occurred in the documentation of audit evidence. On the other hand, it shows that there is a positive relationship between the documentation of the audit evidence and accounting information security culture policies. As the value of this relationship reached at (0.29), and by the value of the coefficient of determination (R square), it shows that the documentation of audit evidence policies interprets the ratio of (8%) of the variances in the accounting information security culture variable. Finally, I discovered that the value of the correlation coefficient between the network security policies and documentation of audit evidence has increased from (0.56) to (0.62), after introducing the accounting information security culture to indicate its impact as a variable rate of regression model.

References

Abdullah, M. A., & Fares, S. A. (2016). The Effect of Electronic Auditing in Reducing the Burden of Electronic Environment Complexity of Accounting Information System on the Auditor. *Research Journal of Finance and Accounting*, *7*(14), 175-187.

Alqadi, F. S. (2017). The Role of Internal Auditing in Controlling the Performance for Jordanian Industrial Companies: Empirical Evidence. *International Journal of Business and Management*, *12*(9), 186. https://doi.org/10.5539/ijbm.v12n9p186

Arens, A. A., Elder, R. J., & Mark, B. (2012). *Auditing and assurance services: an integrated approach*. Boston: Prentice Hall.

Backof, A. G. (2015). The impact of audit evidence documentation on jurors' negligence verdicts and damage awards. *The Accounting Review*, *90*(6), 2177-2204. https://doi.org/10.2308/accr-51072

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. *European Journal of Information Systems*, *18*(2), 151-164. https://doi.org/10.1057/ejis.2009.8

Buccioli, M., Perger, P., Agnoletti, V., Orelli, R. L., Padovani, E., &Gambale, G. (2015). Operating Room Management Accounting and Cost Calculation Model for Operating Rooms. In *Encyclopedia of Information Science and Technology, Third Edition* (pp. 33-43). IGI Global. https://doi.org/10.4018/978-1-4666-5888-2.ch004

Damenu, T. K., & Beaumont, C. (2017). Analysing Information Security in a Bank using Soft Systems Methodology. *Information & Computer Security*, *25*(3). https://doi.org/10.1108/ICS-07-2016-0053

Ghernaouti-Hélie, S. (2007). Cybersecurity Guide for Developing Countries Release.Enlarged edition. ITU-D publication. http://www.itu.int/ITU-D/cyb/publications/index.html

Hai, P. T. (2016). The Research of Factors Affecting the Quality of Audit Activities: Empirical Evidence in Vietnam. *International Journal of Business and Management*, *11*(3), 83. https://doi.org/10.5539/ijbm.v11n3p83

Hamed, H., & Al-Shaer, E. (2006).Taxonomy of conflicts in network security policies. *IEEE Communications Magazine*, *44*(3), 134-141. https://doi.org/10.1109/MCOM.2006.1607877

Mousa, M. S. & Al Qa’qa’a, K. A. (2016). The Barriers Which Face Auditing Profession and Their Impact on the Quality of the Jordanian Auditor's Report. *Research Journal of Finance and Accounting*, *7*(22), 15-27.

Okab, R. (2013). The Expert Systems and Their Role in Developing External Auditor's Performance and Improving Audit Service's Quality in Information Technology Environment in Audit's Offices Located in the Hashemite Kingdom of Jordan. *International Journal of Business and Management*, *8*(17), 129. https://doi.org/10.5539/ijbm.v8n17p129

Peltier, T. R. (2016). *Information Security Policies, Procedures, and Standards: guidelines for effective information security management*. CRC Press.

Romney, M. B., Steinbart, P. J., Mula, J. M., McNamara, R., & Tonkin, T. (2013). *Accounting Information Systems [1st Australasian edition]*. Pearson Australia.

Roscoe, J. T. (1975). *Fundamental research statistics for the behavioral sciences John T. Roscoe*.

Saleh, M. M., Al Amaideh, Z. O., Baniatta, H. M., & Alrjoub, A. M. (2014). The Reflection of Applying New Developed Approaches in Accounting Information System on Investment and Credit Decisions in commercial banks in Aqaba Special Economic Zone. *Asian Journal of Finance & Accounting*, *6*(1), 402-422. https://doi.org/10.5296/ajfa.v6i1.4527

Selamat, M. H., & Babatunde, D. A. (2014).Mediating effect of information security culture on the relationship between information security activities and organizational performance in the Nigerian banking setting. *International Journal of Business and Management*, *9*(7), 33. https://doi.org/10.5539/ijbm.v9n7p33

Simkin, M. G., Norman, C. S., & Rose, J. M. (2014). *Core concepts of accounting information systems*. John Wiley & Sons.

Tan, H. T. (1995). Effects of expectations, prior involvement, and review awareness on memory for audit evidence and judgment. *Journal of Accounting Research*, 113-135. https://doi.org/10.2307/2491295

The National Information Security Technical Committee (NISTC) (2012).*National Information Assurance and Cyber Security Strategy (NIACSS).* National Information Technology Center (NITC). Ministry of Information and Communications.

Uma Sekaran. (2000). *Research methods for business: A skill-building approach*. John Wiley & Sons.

WGITA–IDI. (2014). *Handbook on It Audit for Senior audit Institutions*. Retrieved from http://www.intosaiitaudit.org/WGITA23rd/23rdWGITAMeeting/IT_Handbook.pdf

Whitman, M. E., & Mattord, H. J. (2011). *Principles of information security*. Cengage Learning.

Yoon, K., Hoogduin, L., & Zhang, L. (2015). Big data as complementary audit evidence. *Accounting Horizons*, *29*(2), 431-438. https://doi.org/10.2308/acch-51076

Copyrights