The Impact of the Goals of Information Security Standards to Ensure Information Security

Kulthoom Mansour Al-ghananeem (corresponding author)

Department of Economic and Financial Sciences, Faculty of Finance and Business

The World Islamic Sciences University, Amman, Jordan

E-mail: kghananeem@yahoo.com

Prof. Dr. Mohammed Abed Al-taee

MIS Department, Faculty of Economic and Business Administration Science

Zarqa University, Amman, Jordan

E-mail: mohammed.abed.altaee@gmail.com

Dr. Bassem Khoder Jida

MIS Department, Faculty of Business Administration

Jinan University, Lebanon, Tripoli

E-mail: bassemjida@hotmail.com

Received: January 16, 2014 Accepted: February 19, 2014 Published: April 1, 2014

doi:10.5296/jmr.v6i2.5024 URL: http://dx.doi.org/10.5296/jmr.v6i2.5024

Abstract

The study presents the results of the analysis of the goals of information security to ensure information security through a case study of the income tax department and sales in Jordan. The goal of the analysis is to identify the security situation in the department of information and the development of information system security software and knowledge of the impact of these standards on the security of computerized information systems in this department.

The study sample consists of 360 questionnaires, of which 270 questionnaires subjected to statistical analysis, which accounted for 88%, the researcher has conducted a descriptive study to get to the analytical results and the achievement of the objectives of the study.

The results showed the presence of a positive effect to the goals of the information security standards to ensure information security in this organization, where the information security is characterized by extreme sensitivity to external threats.

Keywords: Confidentiality, Integrity, Availability, Accountability, Auditing, Ensure Information Security

1. Introduction

In spite of everything offered by the information age at the moment such as privileges and services, there are significant challenges focused mostly on information security, whether the conservation and storing information electronically or to maintain the confidentiality of institutions or to ensure the existence of the required information and make it available to everyone equally. This involves information security to protect the assets of regulatory disruption of business processes, and modify sensitive data, or disclosure of confidential information. Information security also describes how to protect the information by maintaining the confidentiality, integrity and availability of information, which is possible to represent the organization's assets, operations, and information. The security can exceed the technical controls and includes people, technology, politics, and processes, and other business objectives (Vacca, 2014).

Accordingly, the information constitutes a strategic resource for the modern institution which should be provided to the required specifications (in terms of accuracy, confidence, concentration, time). Hence the importance of the information system in the enterprise, which is the task of providing this information to all levels of management, and must be so to determine the significance of the information and information system (Alzubairy, 2003).

Ensuring that the elements of information security of all or part depends on the information store protection and their uses (E.Whitman, 2010), and related services, not all information requires confidentiality and ensure the non-disclosure, and not all the information in the facility and one equally important in terms of their access or ensure that no tampering. In other words, the value of information comes from the properties owned, when it changes the characteristics of the information they affect the value of the information in either an increase or decrease is the most common.

Usually, the goals of computer security are: confidentiality, integrity and availability (Cimpa, 2013), and where the researcher added two area to the three areas earlier when talking about the security of computer information to become five, including elements of the previous three and a two accountability and auditing, as described in The following figure:

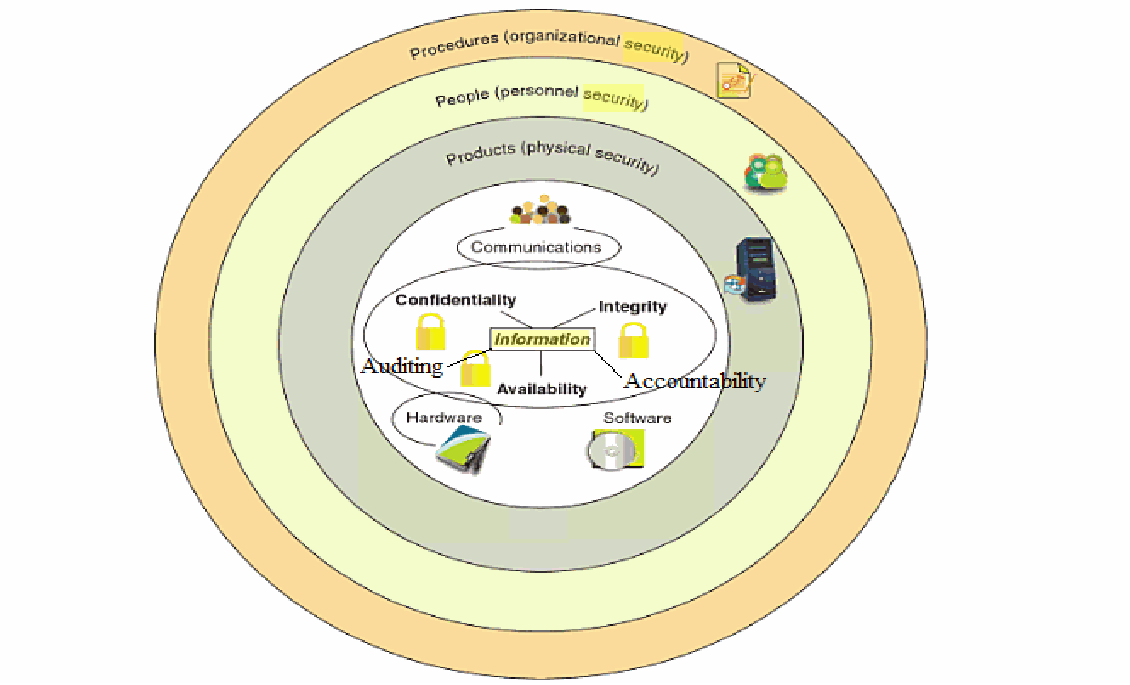

Figure 1. The goals of information security

Source: Introduction to HealthCare Information Technology, 2013.

2. Literature Review

Data Confidentiality

Secret represents a property that allows the recipient of information, reliable confidence as they are represented when targeted to the representation and expression, and uses the pioneers of statistical theory Another term is "reliability," means how much you could count on the information in decision-making (al-Tai, 2012).

The first goal of modern information systems became the systems to ensure that there is reliable as it was expected to face all malicious acts, especially in the face of denial of service. In organizations, secret information is important, especially for personal information about employees, customer information. He defined (Conklin, 2004) the concept of confidentiality which is the information that has been generated and the information systems that ensured supplied, are not accessible only to authorized persons (authorized) to them, and covert measures to protect your access to persons authorized to have. Confirms (al-Tai, 2005) that the secrecy refers to the external properties granted to information involving secrecy and privacy, through the identification of controls and regulations that define the parties are allowed to see it, the tenure it means having the information and control under certain circumstances.

Confirms (Whiteman, 2011) that the secrecy means the case, the status expressive truth and authenticity and depth of information in conformity with the truth and reality, and looking at the authenticity of the information must be true. Shows (Russell, 2006) that the confidential data (Confidentiality) remain obscure to all but be known to people allowed to use it, and determines (Cimpa, 2013) The goal of information security is to protect the integrity and confidentiality, and availability of information on the devices that store, and treatment, and transfer of information, According to identify confidential access to information and disclosed to authorized users access to it (the right people) and prevent access to it by unauthorized persons so (non-suitable persons).

Data Availability

Known site (http://cnss.gov) data availability criteria that provides access and use, upon request by the authorities authorized to access or use, and emphasizes that (Whitman, 2011) who knew that he could not availability, access to information by any user, but it means that the information is available to only authorized user access.

Confirms (Whitman, 2011) that the availability of property information is the property that enables the user access to information without any problems or block access to it, and in any information system serves the objectives, the information must be available when needed.

Thus illustrates (Cimpa, 2013) that the information can not be closed so that no one can access them, otherwise the information will not be useful. Availability of information and make it available to ensure that data can be accessed by authorized persons access to it, and confirms (Conklin, 2004) that the availability means to ensure that the data, or the system itself, is available and is available for use when a person is authorized to access it.

Data Integrity

Indicates (al-Tai, 2012) need to be characterized by a single data accurate enough, and the mean accuracy two different things, namely: to be a single data is correct (Accuracy), a class that reflect their individual data what should express it, and to be accurate (Precision) which is expresses the degree of purity or fineness details when the expression of thing.

In information security, health and safety information means that information does not change and adjusted by persons not authorized to do so, and meant that standard to protect property health information so as not to modify in an unauthorized manner, and illustrates (Whitman, 2011) that the health and integrity of information means that it quality so that the information is complete and correct.

He knew (al-Tai, 2005) the safety information as essential qualities for the perfection of information and cohesion, and they relate to a range of values prevailing in the organization, but realism means a case, the expressing truth and authenticity and depth of information in conformity with the truth and reality.

Shows (Peltier, 2004) that the integrity of the information is aimed at ensuring the information used in making business decisions and maintain appropriate controls to ensure that the information is correct auditable, and repeatable.

Accountability

Accountability within the framework of the goals of information security means bearing the person who access to any information within the system, is responsible for the change that has occurred in the course of arriving to it, whether an employee is responsible for processing information or a customer and this procedure involves taking responsibility for all individuals who have access to the information and have the authority to change information or even access to information. He knew the (Al-Qahtani&Alghathbar, 2009) is intended to ensure that the denial of the person who is connected to the disposal of the information or locations, to deny that he is the one who carried out this act, so have the ability to prove that what may have been an act of someone at a certain time .

Must be the commitment of everyone in the organization to assume all responsibility for the data which it operates and points (F.Tipton & Krause, 2005) to it that there should be accountability for information systems, there should be a mechanism to ensure that the actions taken and the knowledge of the user who work in the system, or network. And see (Griffin, 1993) that the culture of accountability for data based on four pillars: Education, Acceptance, Responsibility, and Communication.

The Possibility of Auditing

And refers (Conklin, 2004) in the world of computer security, audit leads a similar function. In other words, the process of assessing the security situation of the organization compared to the level of standard work in the facility, and to ensure that employees are working in accordance with the procedures and guidelines that can be used, so the audit is also on the data within computers, and is the follow-up work of the staff who work on the existing information systems, and including we are dealing with financial data are processed through the existing computer systems, there should be controlled by the competent authority at the facility. And confirms (F.Tipton & Krause, 2005) that the audit collects information about the safe operation of the requests and the results of these requests for the purposes of this report, including the integration and non-repudiation.

Elements to Ensure The Information Security

Indicates (CIMPA & REVELS, 2013) that the elements of information security includes all the physical components of the equipment and printers for computers and includes all the programs that are running these computers and all the software applications used in the various activities, and mentions (Titi , 2011) are some examples of the use of Information Systems including applications of accounting processes and calculate salaries, or applications, recording and monitoring of students' grades, and includes all the data that is entered directly across different applications and stored in the computer system, including the computer system is also computer networks and all the content of the servers and special equipment for the networks, and includes the computer system of individuals, whether they are users of the system or specialists in the development of programs and the system works.

We will review several elements contribute to ensuring the information security in the environment of the computer systems are as follows:

1 - People security

See (Daod et al, 2001) that are intended to individuals who represent employees, consultants, contractors, technicians and perform all operations and services, and the needs of their presence in numbers and specialties and appropriate skills, experience and motivation occasion. And checks the security of individuals through the use of private stations system computer, there are a large number of people who benefit from the computer and dealing with him, some of them is a measure of experience and competence, and some of them is from the amateur and has a curiosity to know, and some of them is inside work, and some of them is outside, and some of them is with empowered and authorized, and some of them is an intruder, including technical, and maintenance worker, employee and operating systems, and others. From the above it during the parade portion of the segment dealing with the computer, we note that some of them is a first line of defense information systems, and others may represent a major threat to information systems, and sometimes may be the same person authorized to protect the security of information - if abused his powers he did not follow procedures - a danger and a threat to the information.

Accordingly, and in view of the role of the important and influential role of individuals in the provision of security and protection of information it has to be the development of a set of instructions and procedures regarding personnel and who will attract the work, and dealers with the computer, but must also be broadcast awareness among employees and customers about the value and impact of the seriousness of the threats and breakthroughs that they do, or that you may think of them in taking them.

2 - Security Administration

See (Hadi, 2006) that the administration represents the process of keeping the attributes of users, in addition to the definition of the security of a particular resource. This includes activities such as the disposal of the advantages of the arrival of a user or employees leaving the service, change attributes, define a list of what the system allowed for a particular user after the upgrade or transfer. On the other hand confirms (Daod, 2001) that we have to be there management is responsible for this issue is concerned, and organized and planned, and coordinated, and directed in the right direction and define the powers and scope of responsibility, accountability and monitored, and facing the wrong before it happens, if possible, or mitigate its severity, or stops, and facing threats to this system. Thus, it can not deny the role of information security management in warding off danger and threats for information.

3 - The security of computers and systems attached to it

The source and a means of access to information is a computer, devices, and equipment that works each individually, and some of the others devices are working together in the network. Because the elements of computer security are the elements of a coherent, integrated complement each other as parts of the system one, and in order to achieve the security of information, it has to be the care of these devices, and maintained regularly and continuously in an emergency, and to ensure the provision of climate and environment suitable ventilation and heat and moisture, which ensures safety and protection of computers, as well as to be ready to face natural disasters from earthquakes, volcanoes, floods, wars and preparing emergency plan.

4 - The security of communication systems

Leads all the progress and development of systems and means of communication to the evolution of computers, have led ease current connections to facilitate the potential for predators and thieves of the data, as it was possible to transfer data and files through the phone lines, or by wireless communications, and currently through the World Wide Web (Internet). Thus emerged the need to encrypt data sent from one place to another, and the need to develop special procedures for the organization, and to identify ways of communication devices, and data transfer, with the necessity of taking into account the careful and cautious about the means of internal communications for an organization like the wires connecting private networks, devices and accessories.

5 - The security of operating systems and software

After achieving security devices and it is the first part of computer components, we must achieve security for the other half of components of a software and operating systems, it has become impossible to choose computers with systems and its security features can achieve full protection of programs and ways to save passwords, how to manage system operating, and communications systems and utility programs, in addition to the importance of providing security for systems operating on these devices and their data, and through the containment software means to determine the number of users of a particular system, or ways to see data, or modify data, and it also has to be of interest in the development of appropriate procedures while writing systems within the organization to ensure not to leave the door open for the programmer to view some of the data of the organization, with the need for caution and the provision of a leak, or the entry of malicious programs (viruses) into the devices, and by ensuring that the source of the software and tested periodically.

3. Previous Studies

For Arabic Studies did not cover the topic of the goals of security and confidentiality of information dramatically, so it was adopted to study this subject on one of the financial sectors in Jordan and the access to the goals of information security and confidentiality of the information in terms of the possibility of accountability for the information, and the possibility of auditing.

Study (Soltani, 2013) the importance of core values of ethics, integrity and accountability in the laws, and regulations of the European Corporate Governance. The aim of this study is to analyze the laws, regulations and rules of governance that provided by the European Commission and five other European countries (France, Germany, Italy, the Netherlands and the United Kingdom) before and after 2002. The main objective is to study the compatibility of laws and European regulations, especially those issued after 2002 and 2007, has been considered by many important topics such as ethics and corporate behavior, and shareholders' equity, and accountability board. Analyzes show that there have been serious shortcomings in

European corporate governance codes regarding the importance of moral values and integrity in management, and accountability mechanisms.

Focused study (Vasarhelyi, 2012) on the concept of advanced technology, which covers a wide range of technologies used widely in the United States to provide a strategic advantage in the competitive business environment there is a huge amount of information contained in the information systems of the present generation, and some of them are processed on the basis of time real. More importantly, what applies to the actual business transactions? The existence of accurate and reliable is vital and useful for companies, especially in the wake of the recent recession. Thus, they need to ensure the use of information in a timely manner through continuous audit (CA) and monitor continuous monitoring (CM), the methodologies have become more pronounced. To this end, we conducted interviews with 22 managers and 16 internal audit staff, internal audit organizations in 9 internal audits leading to a case study of technology adoption, to assess the development of continuous auditing, monitoring and evaluation of the use of continuous monitoring. Found that many of the companies in the study were already involved in some from of ongoing review or monitoring control while others are trying to adopt more advanced auditing techniques. He also provided a large number of observations on administrative orders, training, and technology absorption, and other issues. According to the model that has done the audit, all the companies were rated among the "traditional audit" phase and the "emerging stage," the absence so far amounted to "continuous auditing" stage. This paper is the first to study the adoption of CA technology in micro-level approach through the interview.

The study confirmed (Hameed, 2011) on the confidentiality of the data and considered a major problem for the health care and medical emergency because it accumulates important information in the system. There is a need multiple levels of security in the field of health care and emergency medical database containing confidential information of different levels. This research addresses the issue of confidentiality through the design and development of a new model for data confidentiality. It offers a view of the sensitivity of the data and suggests areas in encryption to protect sensitive data in different levels. The proposed model protects data transfer using the security policy. As a result of implementation shows that it retains the confidentiality of sensitive data in a certain degree with good performance compared with the normal system and security protocols, and moreover, the cost of encryption and decryption is not high and kept at an acceptable level.

The study provided by (Williams, 2008) that the organizational culture revolves around trust, as is the case in the medical environment, and threats from the inside of malignant and non-malignant alike and difficult to control. Research has shown the international security culture and to raise awareness and necessary technical decisions are not enough to control the threats from the inside. And ensure that all staff bears responsibility for the security of information, particularly in the context of information security governance, a practical solution to the problem of one of the threats from the inside.

He suggested (Hammer, 2007) a more general definition of confidentiality. As an aspect of information security including monitoring information flow, and discuss central aspects of confidentiality and their relation with the standards and policies, and presented in this paper is a language for the expression of such standards and policies, and a number of examples of useful rules of confidentiality.

The study dealt with (Satava, 2006) the subject of financial accounting, auditing, and adopted on the basis of the framework is based on rules. Explained that the recent events, that accountants and auditors concerned with the views of ethical rules and failed to protect investors and stakeholders' interest. This paper describes how the traditions based on the rule checking have become a convenient way that perpetuated the immoral behavior of companies. And concluded in his study to several proposals should be considered to restore confidence and improve the ethical behavior of accountants and auditors.

The study recommended (Boritz, 2005) creates a framework that is broader than that stipulated in the guideline for international control COBIT (ISACA) (Information Systems Audit and Control Association) COBIT recognized widely (information technology control objectives). Witnessed IS views of practitioners on the following issues have been collected through a questionnaire administered during two workshops on the integrity of the information held in Toronto and Chicago: The definition of safety information, the basic features of the cofactors of the integrity of the information and the relative importance of, and the relationship between the integrity of the information attributes and cofactors, experienced people with knowledge of the safety information for selected industries and data stream and their associations with the stages of information processing, key stages of the life cycle of system acquisition/development, and the main components of the system. One of the policy recommendations arising from the results of this study is that the definition of COBIT of safety information that should be reconsidered. Also, should be considered in the context of two layers of the basic features and cofactors.

Study (Flowerday, 2005) that the owners of the companies increasingly rely on digital information. And that includes financial reports, which are generated from many electronic transactions, and is recorded in the books are different. It is expected that this review of financial reports and provide assurances that the information contained in these reports have not been compromised, whether intentionally or unintentionally Auditors. However, it has become important to provide the required safeguards tough with the erosion of traditional audit. Find evidence to prove it in the lapses in corporate governance and recent corporate scandals. One of solutions to this problem is continuous auditing, which helps in verifying the integrity of the information.

4. Objectives of the Study

This study seeks to achieve the following objectives:

- Provide a conceptual framework that includes the goals of information security standards which represents confidentiality, availability, integrity, accountability and the possibility of auditing which is a set of goals that represent the field for the adoption of standards to ensure information security.

-Provide a conceptual framework for the relationship with the most important criteria to ensure information security in organizations in general.

-The nature of computer information system adopted in the Income Tax Department and sales.

-Diagnosis goals of information security standards adopted in the income tax department and sales.

- To reach results that facilitates the task of managers in the Income Tax Department in the promotion and sales computer information systems for the purposes of security standards and confidentiality of the information.

5. Problem of the Study

With the increasing growth of the IT industry a lot of information systems and networks are under the risk of external intrusions and also enabled internet users
to identify programs that help to penetrate the computer systems and easily obtained thus can any user who has little knowledge of the techniques of computer penetration of most computer systems vulnerable. Accordingly, the researcher believes that the efforts made by the department in the design, construction and application of computer information systems are not accompanied by a parallel level of the efforts made to achieve the standards of security and confidentiality of information. From here, the problem can be highlighted through the study of exciting research questions the following:

- Does the income tax department and sales standards to ensure the goals of information security?

- What is the nature of the standards adopted by the income tax department and sales to ensure the security of information?

- What is the impact of the goals of information security in the income tax department and sales to ensure the security of information?

6. In order to solve the problem of the study and seeks to achieve its objectives of this study to test the following hypotheses

The first hypothesis: no statistically significant effect at the level of significance ($\alpha \leq 0.05$) for goals of information security standards to ensure information security.

The second hypothesis: no statistically significant effect at the level of significance ($\alpha \leq 0.05$) standard for confidentiality to ensure information security.

The third hypothesis: no statistically significant effect at the level of significance ($\alpha \leq 0.05$) standard for availability to ensure information security.

Fourth hypothesis: no statistically significant effect at the level of significance ($\alpha \leq 0.05$) standard for Integrity to ensure information security.

Fifth hypothesis: no statistically significant effect at the level of significance (α ≤ 0.05) standard for accountability of the information to ensure information security.

Sixth hypothesis: no statistically significant effect at the level of significance (α ≤ 0.05) standard for auditing of the information to ensure information security.

7. Methodology

The study aimed to examine the impact of appropriate computer information systems at financial institutions to standards to ensure the security and confidentiality of the information in the income tax department and sales, through the assessment of the goals of ensuring the security and confidentiality of the information the adoption of several criteria which confidentiality and availability, and integrity, accountability and the possibility of an auditing. The study adopted a descriptive analytical method to measure and analyzes this effect, in order to draw conclusions and evaluate and test hypotheses and to reach a suitable and practical recommendation. The study comes to complement the efforts of many studies with regard to the approach used and the variables they differentiated from other studies in the environment field application.

To achieve this will be dealt with the way the study and procedures in this section in detail in terms of the method and procedures of the study process, the characteristics of the study sample and the types and sources of data and study tool as well as the procedures for the application of the study.

7.1 Study Population

Based on the problem of the study and its objectives, the targeted community is made up of officers and directors of departments and directors of directorate’s income and sales tax in Jordan's population of about 1477 employees in 20 directorates in the year 2013.

7.2 The Study Sample

The researcher required sample size depending on the size of the total community, according to a study (Sekaran, 2010), which he designed table facilitates decision-making process to determine the sample size required, so it was distributed study tool (questionnaire) at (306) employees, including directors of departments, and six directors of the managers of the income tax and sales in the various governorates of Jordan and recovery (276) questionnaire, was relying on the 270, and it has formed 88% of the total personnel involved in the study.

7.3 Data Source

The researcher used the main sources of information:

1. Secondary sources: The trend in the treatment of the theoretical framework for the search to a secondary data sources, which is in the books and references Arab and foreign-related, and periodicals, articles, reports, research and studies that have addressed the issue of information security, and research and reading on various internet sites.

2. Primary sources: The data was obtained through:

- Survey office. Coverage survey was conducted for the information system the Income Tax Department to indicate the nature of the system and its components and related items.

- The interview was conducted personal interviews with managers and heads of departments sections on the subject of study and personal interviews aimed to answer questions and inquiries researcher on the subject of the study.

- Note: through automatic observation in the workplace (Department of income and sales tax).

-Qquestionnaire: the researcher to design a questionnaire and judged by a group of experts, professionals and academics distributed to the study sample, in order to address the analytical aspects of the research topic.

7.4 Study Tool (Questtionnaire)

1. See literature administrative and previous studies relevant to the subject of the study, and take advantage of them in the construction of the questionnaire and the formulation of its clauses.

2. Showing the questionnaire on a group of experienced arbitrators, and who have, in turn, give some advice and amendments to the questionnaire.

3. In light of the views of the arbitrators was amended some clauses of the questionnaire where the deletion or addition and modification.

4. Were distributed (306) questionnaire and recovery (276) questionnaire, which represents a good percentage of the target sample.

7.4.1 The Questionnaire Included Three Main Sections

Section 1: It is a personality trait for respondent (sex, age, educational qualification, specialization, experience, career level, Job Title, number of hours of daily use for computer).

Section 2: which is a measure paragraphs standards to ensure the goals of information security, and consists of 25 items distributed on five key criteria:

The first criterion: Data confidentiality, consists of (5) variables.

The second criterion: Data availability, consists of (5) variables.

The third criterion: Data integrity, consists of (5) variables.

The fourth criterion: accountability, consists of (5) variables.

The fifth criterion: Possibility of auditing, consists of (5) variables.

Section 3: a measure to ensure the security of the paragraphs of information, and consists of 16 items distributed on the five key elements to ensure information security.

7.5 Statistical Methods Used in the Study

The researcher unloaded the questionnaire and analysis through statistical analysis program Statistical Package for the Social Sciences (SPSS 18), were used nonparametric statistical tests, and this is due to the Likert scale is ordinal scale, has been the use of statistical tools the following:

1.Standards Descriptive Statistic Measures in order to describe the characteristics of the study sample, depending on the percentages and frequencies, the arithmetic mean and standard deviations, This command is used mainly for the purpose of knowing what variable repeat classes.

2. Test Cronbach's Alpha to determine the stability of the paragraphs of the questionnaire.
3. Test Principle Factor Analysis is used to calculate the internal consistency of the questionnaire, and through it is determined by the number of variables involved through the analysis of the data in this way.

4. Pearson correlation coefficient matrix to measure the degree of correlation. This test is used to examine the relationship between the variables in the case of nonparametric data.

5. Sign Test to determine whether the average degree of response had reached a degree of neutrality which is 3 or not.

6. Normal Distribution test, test was used (Smirnov-kolmogorov) to indicate the extent of the data follow the normal distribution.

7. Strength test model, the test was used (Multicolleniarity) to indicate the strength of the association between variables without the presence of overlap between them.

8. Simple Regression analysis to test the hypothesis of the first hypothesis.

9. Multiple Regression analysis to test the hypotheses of the study the second, third, fourth and fifth.

7.6 The Model Variables

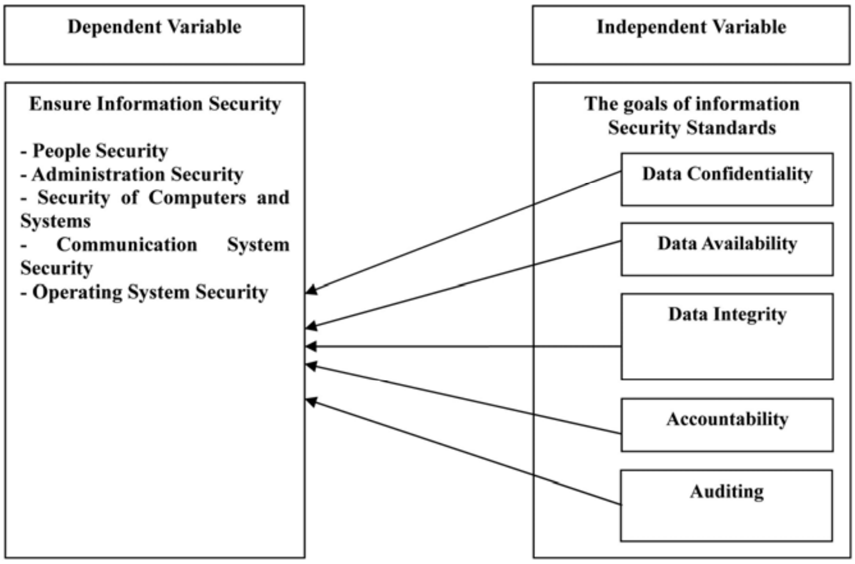
Dependent Variable
Independent Variable
Ensure Information Security
- People Security
- Administration Security
- Security of Computers and Systems
- Communication System Security
- Operating System Security
The goals of information Security Standards
Data Confidentiality
Data Availability
Data Integrity
Accountability
Auditing

Figure 2. Represents a model study, prepared by the researcher

Through a model study shows that there are five criteria for the goals of ensuring the security of information, where it represents the independent variables and to ensure the security of information representing the dependent variable.

8. Experimental Results and Discussion

This section includes a detailed analysis of the data and a presentation of the results through processors Statistics conducted on the sample of the study, and then analyze and discuss the results and determine the extent of statistical significance.

8.1 Description statistical sample of the study according to the characteristics and personal characteristics

This section describes the demographic characteristics and functional for the study sample which represents sex, age, educational qualification, specialization, and practical experience, and functional level, and job title. To illustrate the characteristics of the study sample description, has been found frequencies and percentages for demographic variables and functional for the study sample as follows:

1 - Description of demographic characteristics. The table (1) shows frequencies and percentages for demographic variables of the study sample and of sex, age, qualification, and specialization.

Table 1. Frequencies and percentages for demographic variables of the study sample

Variable	Category	Redundancy	Percentage
Gender	Male	205	75.9
	Female	65	24.1
	Total	270	100
Age	Less than 30	30	11.1
	30- less than 40	149	55.2
	40-less than 50	69	25.6
	Greater than or Equal 50	22	8.1
	Total	**270**	**100**
Academic Qualification	Diploma	39	14.4
	Bachelor	191	70.7
	Master	38	14.1
	Doctorate	2	0.70
	Total	**270**	**100**
Major	Computer	38	14.1
	Business Administration	19	7.0
	Accounting	170	63.0
	Otherwise	43	15.9
	Total	**270**	**100**

Shown in Table (1) that males make up (75.9%) of the study sample, while the form females accounted for 24.1% of the sample, and this may be due to the above men for women to the labor market may be due also to the reluctance of women to work in Income tax for the difficulty of the work and the length of periods of daily attendance, and the need for field work. With respect to the age of the sample, we find that age group (30 - less than 40 years old) are the largest category, which accounted for 55.2%, while the age group (50 years and older) are the least and by (8.1%), and this is consistent with the idea of attracting young people to carry out the duties and functions in the Income Tax Department, and the age groups are usually large handles administrative work the upper and middle and thus characterized by a lack of issue in accordance with the administrative hierarchy in any organization. On the other hand data show (Table 1) that the percentage of holders of BA degree is (70.7%) so they make up the majority of the sample, this corresponds to the general trend in both the public and private sectors, which are required in the process of appointment and the employee, get a bachelor’s degree as a minimum.

When searching in the subspecialties of the study sample, we find that the ratio of specialists accounting constitute the majority of the sample at a rate (63.0%), and this is consistent with the need for income tax specialists accounting because they are the most knowledgeable about the law of the tax and how to measure and assess the tax, and determine the size of the tax base and the discovery of fraud and tax evasion.

2 - Description of functional characteristics. The table (2) shows frequencies and percentages for functional variables of the study sample and of practical experience, and functional level, and job title, and the number of hours of daily use of the computer.

Table 2. Frequencies and percentages for functional variables of the study sample

Variable	Category	Redundancy	Percentage
Experience	3 Months – less than 1 Year	2	0.7
	1- less than 2 year	3	1.1
	2- less than 5 years	20	7.4
	5- less than 10 years	74	27.4
	10- less than 15 years	81	30.0
	greater than or equal 15	90	33.3
	Total	**270**	**100**
Career Level	Manager	11	4.1
	Assistant Manager	6	2.2
	Head of Department	26	9.6
	Head of Division	26	9.6
	Supervisor	37	13.7
	Auditor	135	50.0
	Writer	29	10.7
	Total	**270**	**100**
Title Job	Administrative	133	49.3
	Technician	95	35.2
	Programmer	27	10.0
	Data entry	15	5.6
	Total	**270**	**100**
Number of hours used computer daily	Less than hours	2	0.4
	Hour - less than 3 hours	34	12.6
	3 hours - less than 5 hours	71	26.3
	5 hours - less than 8 hours	164	60.7
	Total	**270**	**100**

Notes from the table (2) that the respondents have practical experience relatively high, where she was a class experience (15 years) is the largest category compared with other groups and by as much (33.3%), followed by the categories of expertise relatively high, which is compatible with the idea that the work in Income Tax Department requires high expertise and skills among workers. In the same way, we find that the sample of auditors form the highest percentage, with a percentage (50.0%) of the sample size, and this reflects the nature of the work in the Income Tax Department that are consistent with the work of the auditor, as can be confirmed by the auditors in assessing the merits of the tax. When search Job Titles prevailing in this Directorate notes that respondents may be divided between the administrators and technicians, to reflect the need for the two designated functional to do daily chores emerging more than others.

Finally, with regard to the computerization of the work in this Directorate, table (2) shows that the largest category of the number of hours the use of Computer is (5 hours - less than 8 hours), where the percentage (60.7%), and this period is approximately the majority of working hours daily in Income Tax Department, may be due to the fact that all the information in the organization have been made to the computers and therefore do any work involving the use of Computer.

8.2 Analysis of the Paragraphs of the Study

The researcher tested the paragraphs of the study using a test signal to see if the average response had reached a degree of neutrality or not a 3, which corresponds to a moderately (neutral) as a measure of the Likert. Depending on the value of Sig. (P-Value) for each paragraph of the questionnaire, if Sig> 0.05 (Sig greater than 0.05), according to the results of the SPSS program, it would be in this case the average views of respondents about the phenomenon under study does not differ materially from OK degree.

It is a medium 3 (neutral), but if Sig<0.05 (Sig less than 0.05), the average views of the sample differs substantially from the approved medium degree (neutral), and in this case could determine whether the average answer is increased of decreased significantly from approval medium (neutral).

Through the value of the test, If the signal is positive what this means is that the arithmetic mean of the answer over medium degree of approval (neutral), and vice versa.

8.2.1 Description Variables of the Study

This section of the study and a description of the variables of the study, which was calculated averages and standard deviations of the responses in order to judge the degree of approval, and when determining the relative importance of each paragraph, and the results were as follows:

First: The Goals of Information Security Standards (independent variables)

Table 3. Shows the averages and standard deviations, grade and importance of each criterion and the goals of ensuring information security

No.	Dimension	Mean	Standard deviation	Rank	Relative Importance
1.	Data Confidentiality	3.53	0.61	5	High
2.	Data Availability	3.77	0.53	3	High
3.	Data Integrity	3.97	0.85	1	High
4.	Accountability	3.67	0.71	4	High
5.	Auditing	3.84	0.55	2	High
The Goals of Information Security Standard		3.76	0.133		High

The results of the Table (3) that the level of standards of the goals of ensuring the security of the information in terms of the relative importance of a high, reaching the arithmetic mean (3.76) with a standard deviation (0.133), and also showed a table that standard (Data Integrity) came in first place with an average (3.97) and standard deviation (0.85) and high relative importance, while the standard (Data Confidentiality) ranked the recent average (3.53) and standard deviation (0.61) and high relative importance.

Second, ensure the security of information

The variable of the study, which was calculated averages and standard deviations of the responses in order to judge the degree of approval, and determine the relative importance of each element of ensuring the security of information, and the results were as in the following table:

Table 4. Shows the averages and standard deviations, grade and each relative importance element to ensure information security

No.	Dimension	Mean	Standard deviation	Rank	Relative Importance
1.	People Security	3.65	0.823	3	High
2.	Administration Security	3.25	0.68	5	Medium
3.	Security of Computers and Systems	3.62	0.755	4	High
4.	Communication System Security	3.98	0.70	2	High
5.	Operating System Security	4.16	0.71	1	High
Ensure Information Security		3.73	0.056		High

The results of Table (4) that the level of scale ensure the security of information in terms of the relative importance of a high, reaching the arithmetic mean (3.73) with a standard deviation (0.056), and also showed a table that axis (the security of operating systems and software) came in first place with an average (4.16) and a standard deviation (0.71) and high relative importance, while the axis (Security management) ranked the recent average (3.25) and standard deviation (0.68) and the relative importance of medium.

8.2.2 Believe Questionnaire

Honestly questionnaire intended to measure what questions questionnaire developed to measure in order to achieve the objectives of the study and answer the questions and hypotheses, the researcher has verified the validity questionnaire in two ways:

1. Virtual tool (opinion of arbitrators)

Has been questionnaire in primary form a group of arbitrators composed of 14 faculty members at various universities specializing in the field of scientific research and management information systems and applied statistics, has responded by seeking the views of the gentlemen of the arbitrators, and in the light of those views have been disposed of some paragraphs and add some and modify others, and thus came out the questionnaire in its final form.

2. Internal consistency of the questionnaire

meant the internal consistency of the consistency of each paragraph of the questionnaire with the standard to which it belongs this paragraph, have been calculated internal consistency of the questionnaire by calculating the correlation coefficients between each paragraph of the areas of the questionnaire and the total score of the standard to which it belongs this paragraph.

And is determined by the number of variables involved by analyzing the data in a way the main factors Principle Factor Analysis, to extract the results of factor analysis were as follows:

Table 5. The results of factor analysis

Variable	Factor	Extraction
Data Confidentiality	0.796	0.688
Data Availability	0.608	0.741
Data Integrity	0.627	0.857
Accountability	0.677	0.745
Auditing	0.843	0.828
The Goals of Information Security Standard	0.796	0.829
Ensure Information Security	0.668	0.739

Depending on the factor analysis shows the value of any variable less than (0.40) is deleted from the study. The above table indicates that all values were greater than (0.40) and therefore all the variables are considered highly credible in the process of analysis and get results.

8.2.3 The Stability of the Questionnaire

Intended steadfastly questionnaire to give the same result if the re- distribution of the questionnaire more than once under the same circumstances and conditions, or in other words, means that the stability of the questionnaire to give readings converged when every time you use and do not change dramatically as if it were re- distributed to the members of the sample several times during the certain periods of time, because the tool fluctuating unreliable and do not take their results, and therefore will be the results of the study are not comforting and misleading. There have been a researcher from the stability of a questionnaire study using the Cronbach's Alpha to calculate the coefficient of internal consistency for measuring the stability of the questionnaire, and the results were as shown in the following table:

Table 6. The values of coefficient of internal consistency of the paragraphs of the goals of information security standards

No.	Dimension	Alpha value
1.	Data Confidentiality	0.632
2.	Data Availability	0.626
3.	Data Integrity	0.622
4.	Accountability	0.891
5.	Auditing	0.741
6.	The Goals of Information Security Standard	0.874

Note that the values of coefficient of internal consistency, Cronbach's alpha for paragraphs standards of the goals of information security standards ranged (0.622-0.891), in addition to the alpha value of all the paragraphs were (0.874), and thus all values greater than (0.60) is an indication of consistency between the paragraph study tool, and reliability study tool and the possibility for a reliable statistical analysis.

Table 7. The values of coefficient of internal consistency of the paragraph to ensure information security

No.	Dimension	Alpha value
1.	People Security	0.614
2.	Administration Security	0.701
3.	Security of Computers and Systems	0.609
4.	Communication System Security	0.641
5.	Operating System Security	0.620
6.	Ensure Information Security	0.609

Note that the values of coefficient of internal consistency, Cronbach's alpha for the paragraph to ensure the security of information ranged (0.609-0.701), in addition to the alpha value of all the paragraphs were (0.609), and thus all values greater than (0.60) is an indication of consistency between the paragraph study tool, and reliability study tool and the possibility for a reliable statistical analysis.

8.2.4 Test Appropriate Form

To test the suitability of the study data for the analysis of linear regression and parametric tests, it has been tested normal distribution, and linear and multiple linear correlation, and autocorrelation.

1 - Test Normal Distribution (Normality)

Used in this regard, two types of tests to make sure free sample of extreme values, and they are distributed naturally, and these two tests are the Kolmogorov-Smirnov & Shapiro-Wilk, where the base states that the variable follows a normal distribution if the Sig is greater than 5%, (Gujarati , 2003) and the results were as shown in the following table:

Table 8. The normal distribution test

Variable	Kolmogorov-Smirnov(a)			Shapiro-Wilk		
	Statistics	**df**	**Sig.**	**statistics**	**df**	**Sig.**
Data Confidentiality	0.111	270	**0.200**	0.952	270	**0.208**
Data Availability	0.132	270	**0.200**	0.969	270	**0.521**
Data Integrity	0.167	270	**0.099**	0.938	270	**0.091**
Accountability	0.152	270	**0.087**	0.931	270	**0.058**
Auditing	0.141	270	**0.148**	0.958	270	**0.298**
The Goals of Information Security Standard	0.142	270	**0.141**	0.967	270	**0.478**
Ensure Information Security	0.117	270	**0.200**	0.964	270	**0.419**

We note from the above table that all the values for the test revealed a level of significance greater than 0.05 and this is proof that all values are distributed in a normal and there are no outliers could affect the model within the sample.

2 - Testing of multi-linear correlation (Multicollinearity Tests):

I have been using correlation coefficients Pearson to detect a problem link multiple linear between the variables of the study, which showed the values of the correlation coefficient between the dependent variable (information security) and the independent variables were all values are statistically significant and at a level of significance 0.01 (**), and is an indication of the presence of linear relationship between the variables of the study sample.

The highest correlation between independent variables is (0.648) between the two variables (risk control) and (security policies) while the values of correlation coefficient between the other independent variables was less than that, and this indicates that there is no visible link multiple linear between independent variables, where is the link you up to the top of (0.80) an indication of the existence of this problem, so we say that the sample is free from the problem of multi-linear correlation higher.

Table 9. Correlations between variables

	Ensure Information Security	Data Confidentiality	Data Availability	Data Integrity	Accountability	Auditing
Ensure Information Security	1					
Data Confidentiality	0.351	1				
Data Availability	0.238	0.607	1			
Data Integrity	0.267	0.615	0.525	1		
Accountability	0.237	0.526	0.407	0.516	1	
Auditing	0.359	0.566	0.504	0.610	0.578	1

8.2.5 Test Hypothesis of the Study

The first hypothesis was subjected to simple linear regression and the results were as follows:

Table 10. Results of simple linear regression analysis of the goals of information security with ensure information security

Dependent Variable	**R**	**R^2**	**F**	**Prob (F-statistics)**	Regression coefficient				
					Statement	**β**	The standard error	t	Sig F*
Ensure information security	**0.411**	**0.169**	**54.41**	**0.000**	The Goals of Information Security	**0.411**	**0.043**	**7.37**	0.000

The results of the above table that the effect of the independent variable (The Goals of Information Security) on the dependent variable (ensure information security) is a statistically significant effect, where the F value calculated is (54.41), and the level of significance (Sig F = 0.000), which is less than (0.05), while the correlation coefficient (R = 0.411) refers to the positive relationship between the two variables, in addition to the value of the coefficient of determination was (R^2 =0.169) which indicates that 16.9% of the variance in (ensure information security) can be explained During the variation in the (the goals of information security), with all other variables constant.

The regression coefficient (β=0.411) refers to the direct impact for goals of information security to ensure the security of information is a significant effect, where the value of t when this criterion (7.37) and the level of significance (Sig=0.000), and therefore reject the hypothesis, which provides that:

There are statistically significant effects at the level of significance ($\alpha \leq 0.05$) for the goals of information security to ensure the security of the information.

The rest of the hypotheses have been subjected to multiple linear regression analysis, and the results were as follows:

Table 11. As a result of the regression analysis of the goals of information security

Dependent Variable	**R**	**R^2**	**F**	**Prob (F-statistics)**	Regression coefficient				
					Statement	**β**	The standard error	t	Sig F*
Ensure information security	**0.403**	**0.162**	**5.974**	**0.000**	Data Confidentiality	**.145**	**.065**	**2.232**	**0.027**
					Data Availability	**-.012**	**.058**	**-0.211**	**0.833**
					Data Integrity	**-.006**	**.049**	**-0.112**	**0.911**
					Accountability	**-.017**	**.044**	**-0.375**	**0.708**
					Auditing	**.150**	**.061**	**2.486**	**0.014**

The results (Table 11) that the effect of the independent variables (the goals of information security standards) on the dependent variable (ensure information security) is a statistically significant effect , where the F value calculated is (5.974), and the level of significance (Sig F = 0.000), which is less from (0.05), while the correlation coefficient (R = 0.403) refers to the positive relationship between the independent variables and the dependent variable, in addition to the value of the coefficient of determination was (R^2 = 0.162) which indicates that (16.2%) of the variance in the (ensure information security) can be explained by the variation in the (the goals of information security standards).

The regression coefficients (β) refers to the direct impact of a standard confidentiality of information and the possibility of auditing to ensure that information security is a significant effect, where the value of t at the standard confidentiality of the information is (0.145) and the level of significance (Sig = 0.027), while the value of t when standard is the possibility of auditing (0.150) and the level of significance (Sig = 0.014), did not impact the rest of the standards had a significant effect, although the standards combined impact was significant.

Accordingly, we reject the main hypothesis and accept the alternative hypothesis, which states that:

There are statistically significant effects at the level of significance ($\alpha \leq 0.05$) for the goals of information security to ensure information security.

And to identify any of the criteria for the goals of information security has had a prominent impact in ensuring the security of information has been applied stepwise linear regression analysis, and the results were as follows:

Table 12. Results of stepwise regression analysis to show the impact of the goals of information security in ensuring the security of information

Sample	Ensure information security	β	Sig*	R^2	The standard error	F	Sig*
1	Auditing	0.208	0.000	0.359	0.326	23.400	0.000
2	Auditing Confidentiality	0.137 0.129	0.009 0.015	0.402	0.321	15.091	0.000

When reviewing the table (12), we find that the first model resulting from stepwise regression indicates that the (Auditing) has been interpreted as representing (35.9%) of the total variance in happening (ensure information security), has increased the proportion of the total variance explanation happening in (ensure information security) to a rate (40.2 %) , and so when you add the (Data Confidentiality) to (Auditing). Has shown the value of β that the direct impact of the variables in the models 1 and 2 and has a positive effect is statistically significant.

In addition to the above, the results of the analysis indicate the absence of the influence of each of the standard (Data Availability, and Data Integrity, and Accountability) to ensure the security of information, and this is compatible with multiple regression analysis.

9. Conclusion

In light of the results of the analysis and testing of hypotheses, it is shown that the goals of information security to ensure the information security, which represents the data confidentiality, data availability, data integrity, accountability , and the possibility of auditing have a positive impact on ensuring the information security and when you search in computerized information systems security in the income tax department and sales, we find that security is one of the central aspects of confidentiality and their relationship with other standards and thus agree with the (Hammer, 2007), and agreed with us also (Hammed, 2011) that the confidential information is a major problem and we need to keep the data, and for the standard of the availability and use of information has been agreed with (Vasarhelyi, 2012) to ensure the use of information in a timely manner, either for the rest of the criteria standard integrity of the information we note from the results of the analysis we came to an agreement with (Flowerday, 2005) that the integrity of the information is done through a standard audit, was reached that the income tax department and sales adopted standard of accountability and thus disagree with us (Soltani, 2013) which showed that the analyzes carried out that there is a severe lack of European corporate governance regarding the importance of information and problem appear in the moral values and integrity in the administration and accountability mechanisms.

The results of our study are consistent with (Williams, 2008) that all employees are responsible for information security, in particular in the context of information security governance.

The study also found many of the observations regarding the goals of information security standards, namely:

- Are not exposed credibility of the information available in the income and sales tax to the attack by the workers, for considerations relating to the existence of a system of deterrent penalties, against the employee aggressor on information security.

- Lack of awareness about the trading password for each employee to enter into a system of income tax and sales with coworkers.

- That the skills and experience high among employees (workers who have the experience of 15 years and over are the largest category) , along with heavy use of the computer by these employees (most of the working hours spent by staff to enter data into the computer and extract other data or estimate data or sent correspondence or information other related work between the different branches of the Department of Home) leads to the conclusion that the adoption of ensuring the security of the information in this circuit is characterized by great sensitivity toward internal threats, which requires a focus on the potential risks arising from them.

References

Boritz, J. E. (2005). IS practitioners' views on core concepts of information integrity. *International Journal of Accounting Information Systems*, *6*(4), 260-279. http://dx.doi.org/10.1016/j.accinf.2005.07.001

Cimpa, M., & Revels, M. (2013). *Introduction to HealthCare Information Technology*. Cengage Learning, Boston, Electronic Version.

Conklin, A., White, G., Cothren, C., Williams, D., & Davis, R. L. (2004). *Principles of Computer Security*, McGraw-Hill Technolog Education, USA.

Dawood and Mashhadani, Sarhan Suleiman, Mahmoud Abdel-Moneim. (2001). *Computer Security and Information*, Dar Wael for publication, Jordan - Amman.

Flowerday, S., & von Solms, R. (2005). Continuous auditing: verifying information integrity and providing assurances for financial reports. *Computer Fraud & Security*, *2005*(7), 12-16. http://dx.doi.org/10.1016/S1361-3723(05)70232-3

Hameed, S. A., Yuchoh, H., & Al-khateeb, W. F. (2011, May). A model for ensuring data confidentiality: In healthcare and medical emergency. In *Mechatronics (ICOM), 2011 4th International Conference On* (pp. 1-5). IEEE.

Hammer, J. H., & Schneider, G. (2007, August). On the definition and policies of confidentiality. In Information Assurance and Security, 2007. IAS 2007. *Third International Symposium on* (pp. 337-342). IEEE.*h ttp;//www.cnss.gov/Assets/pdf/cnssi_4009.pdf*, Date Access 24/7/2012. income and sales tax, http://www.istd.gov.jo, Date Access 1/12/2013.

Mohammed al-Tai. *(2005) Information Security: hack areas and the mechanism of reinforcement,* Arab Journal of Security Studies and Training, No. 40.

Mohammad Hadi. (June 2006). Trends and transparency of information security in light of the e-government. *cybrarians journal.*

Peltier, T.R. (2004). *Information Security Policies and Procedures*, Auerbach Publication, United States of America, page 293. http://dx.doi.org/10.1201/9780203488737

Russell, D., & Gangemi, G.T. *(2006). Computer Security Basics,* O'Reilly Media, United State, Electronic Version, 2nd Edition, Page 9.

Satava, D., Caldwell, C., & Richards, L. (2006). Ethics and the auditing culture: rethinking the foundation of accounting and auditing. *Journal of Business Ethics*, *64*(3), 271-284. http://dx.doi.org/10.1007/s10551-005-0556-y

Sekaran, Uma, & Bougie, Roger *(2010). Research methods for business: A skill-building approach,* New York: John Wiley & Sons Inc., 5th Ed.

Soltani, B., & Maupetit, C. (2013). Importance of core values of ethics, integrity and accountability in the European corporate governance codes. *Journal of Management & Governance*, 1-26.

Tipton, H.F., & Krause, M. (2005). *Information security management handbook*, *2*, AUERBACH PUBLICATIONS, United States of America, 5th edition.

Titi, kheder mesbah. (2011). *Knowledge Management: Challenges, technologies and solutions*, Dar Hamed publication and distribution, Jordan – Amman.

Vacca, Johnr. (2014). *Managing Information Security*. Elsevier Inc, London, Electronic Version, Second edition.

Vasarhelyi, M. A., Alles, M., Kuenkaikaew, S., & Littley, J. (2012). The acceptance and adoption of continuous auditing by internal auditors: A micro analysis. *International Journal of Accounting Information Systems*. http://dx.doi.org/10.1016/j.accinf.2012.06.011

Whitman, M.E., &Mattord, H.J. (2011). *Road Map to Information Security: For IT and InfoSec managers*, Course Technology, Boston, Electronic Version.

Whitman, M.E., &Mattord, H.J. (2010). *Management of Information Security,* Technology Cengage Learning, Australia, Electronic version, 3rd edition.

Williams, P.A. (2008). In a trusting' environment, everyone is responsible for information security. *Information Security Technical Report, 13*(4), 207-215. http://dx.doi.org/10.1016/j.istr.2008.10.009

Zuberi Rabeh. (2003). The role of information systems in the development of the competitiveness of the institution," the first national forum on "Algerian economic enterprise and the challenges of the new economic climate. the University of Algiers, an electronic copy.