

Role for Internal Auditor to Cope with IT Risks and IT Infrastructure in Jordan Commercial Banks

Atallah Hosban¹ & Mohammed Naser Hamdan²

¹ Irbid National University, Jordan

² Al Albeit University, Jordan

Correspondence: Atallah Hosban, Irbid National University, Jordan. E-mail: aalhosban@gmail.com

Received: December 29, 2014

Accepted: January 26, 2015

Online Published: February 27, 2015

doi:10.5539/ijbm.v10n3p295

URL: <http://dx.doi.org/10.5539/ijbm.v10n3p295>

Abstract

This study aims to provide assurance to senior management on the adequacy of the controls to ensure the IT infrastructure was planned, managed and maintained to support efficient operations and analyze risk assessment and know the role of it auditors to deal with risks which threats attain strategic objectives. The study population consists of the internal auditors in Jordan commercial banks. the most results : Audits can focus on such major IT assets as ERP systems and help management to make rational decisions in investing in IT assets to attractive new customers and make core competences for company, technology infrastructures have continued to grow in size and complexity. Servers, storage area networks (SANs), and network attached storage (NAS) and Audit risk assessment Evaluation of risks related to the value drivers of the organization, covering strategic, financial, operational, and compliance objectives, Audit risk assessment Evaluation of risks related to the value drivers of the organization, covering strategic, financial, operational, and compliance objectives. and most recommendations are An audit to verify that IT management has developed an organizational structure and procedures to ensure a controlled and efficient environment for information process and risk assessment is the identification and analysis of relevant risks to the achievement of an organization's objectives, important to care risk assessment is the identification and analysis of relevant risks to the achievement of an organization's objectives.

Keywords: internal auditor, IT risks, commercial banks, infrastructure IT

1. Introduction

Technological developments underlined the need for specialization in a particular field, which means the possibility of finding familiar with the work of the audit and information technology people, and they have several skills so that they can quickly identify opportunities and risks of the technology on the company, and in general to be the availability of specialists in accounting and auditing work, especially in the field of information technology whether for internal or external auditor.

Computer has become in the present day the primary means to process data in various aspects of economic activity in the public and private institutions, and with the increasing use of computers and therefore the information technology and the growing realization that the data relied upon by the continuation of institutional operations and the certainty that the information derived from these data paint a picture of the organization and its environment and its future, fears of a lack of adequate control over the computer business and technology the widespread use of information technology in the public and private sectors, has led to the need to keep up with the internal control requirements of the technology system. With the growing use of computers, the public shareholding companies worked on electronic data processing, so that information technology has become part of the company's environment, and to continue to information systems to their impact on the operations of the various companies and data processing imposes on the internal control systems keep pace with these developments. As the most attractive sectors of the technology public shareholding companies, so this study was to look at the extent of the internal control systems of these companies in response to the requirements of information technology

1.1 Problem Study

1)-What is the role of the internal auditor in dealing with the infrastructure of information technology in

commercial banks in Jordan?

2)-What is the role of the internal auditor in dealing with the risks of information technology in commercial banks in Jordan ?

1.2 Hypothesis Study

1)-There is no role of the internal auditor in dealing with infrastructure tools of information technology in commercial banks.

2)-There is no role of the internal auditor in the Jordanian commercial banks in dealing with information technology risk.

1.3 Objectives Study

1)-Identify the infrastructure developments of information technology and linked work environment Internal Auditor

2)-Identify the risks of using information technology tools work environment internal auditor and how to mitigate them

3)-Find a link between IT tools and work of internal auditor tools through Applied Study on Jordanian commercial banks

1.4 Importance Study

Is consistent and clear goals for the company put a prerequisite for risk assessment. Intended to assess the risk identification and analysis of the relationship of risk associated with the achievement of specific performance in the strategic plan goals. In determining these risks are analyzed to identify the impact when the application of information technology, because technology punctuated by constant changes according to the company conditions, so it is necessary to establish clear mechanisms to identify these risks resulting from these changes and how to handle them. The technological developments make permanent accounting software need to be modified and development to suit the nature of the company's business and developments in the environment in which it operates, which means the need to rely on providers of programs and increase the possibility of guaranteeing them and modify them if necessary, in addition to increasing the period of maintenance.

Society and the study sample

The study population of Jordanian commercial banks traded on the Amman Stock Exchange Securities Exchange questionnaires were distributed to the internal auditors using simple random sample.

1.5 The study Methodology

1)-Secondary sources: through the use of references and books and previous studies to cover the theoretical framework for the subject of the study

2)-Primary sources: through the design of a questionnaire containing variables and hypotheses of the study and distributed to internal auditors to draw statistical results

1.6 Previous Studies

Alotaibey (2014) Assess the level of governance of information technology in Taif University using Koept scale. The purpose of the study to assess the level of governance of information technology in Taif University using Koept scale, and thus assess Methodology used in the organization of this important resource for the University and measure the rules that have been developed in order to ensure greater efficiency and effectiveness of the techniques Used and the face of a Sister papers and infringement of technical resources of the university, is performed by the study in the questionnaire that was designed for this The purpose building on many of the father of a former anchored in this regard, and provide important information about the level of governance of information technology At the university, benefiting Take a PL-makers and users of this important resource. Be the father of the community of all employees in Taif University who use information technology in the performance of their business, has Numbered (1252), was chosen as a random sample of 104 employees reporting, Set of results that the most important information technology in Taif University Tate galore where gubernatorial that technology dimensions according to the measure Koept, and of: planning directions, and the organization of human resources, and the acquisition of information infrastructure, and application Take a year of rate Administrative, and improve the services provided to customers better, and to provide a specific level of control and the establishment of a sustainable evaluation process.

Study of AL-Johar "The Risk Impact of the Use of Technology in the Job Quality of External Auditors Field

Study in Some of the Jordanian Auditing Offices". The scientific and technical developments are important characteristic of our times, and also the continuity of their occurrence rate and their impact on our lives. Hence, organizations and individuals can't ignore the impact of those developments, especially those associated with information technology. Therefore, most of the organizations started to take advantage of these enormous techniques in their various work areas, including accounting area. With the employment of these techniques, the auditing offices started to face great and growing loads and it has become essential to adapt to these new techniques for operation and areas of usage. In the light of the electronic operating system, the auditor is therefore compelled to understand the hardware of the computer, programs and the electronic operating systems to the extent that enables him/her to plan the auditing process and understand the effects of the use of information technology in auditing. Due to the responsibilities endured by the auditor including reduction and in the light of using technology he/she encounters new risks that may affect his/her performance and responsibility. Therefore, the researcher's choice fell on this topic to shed some light on the dimensions of the impact of information technology in auditing, the types of the potential risks that can be encountered, how can these risks affect the standards of quality of auditing and testing that in a sample of the auditing offices operating in Jordan. The results of the research showed that most of the risks that can be encountered are the risk of exposure due to the inadequacy of regulatory procedures associated with the use of technology and most standards of quality of profession affected by risks of technology are efficiency and merit (Kareema AL-Johar, 2010).

Study of Janvrin (2009) An Investigation of Factors Influencing the Use of Computer-Related Audit Procedures provide data on the extent to which computer-related audit procedures are used and whether two factors, control risk assessment and audit firm size, influence computer-related audit procedures use. We used a field-based questionnaire to collect data from 181 auditors representing Big 4, national, regional, and local firms. Results indicate that computer-related audit procedures are generally used when obtaining an understanding of the client system and business processes and testing computer controls. Furthermore, 42.9 percent of participants indicate that they relied on internal controls; however, this percentage increases significantly for auditors at Big 4 firms. Finally, our results raise questions for future research regarding computer-related audit procedure use.

1.6.1 Difference in the Current Study, All Previous Studies

- The current study is based on linking information technology with the work of the internal auditor environment.
- The current study is based on the infrastructure of information technology with the risks of dealing with it through the internal audit work environment.
- The current study focused on the internal auditors in the banking sector in Jordan, which is one of the sectors most widely used tools for IT.

2. Theoretical Framework of Study

The rapid development of information technology stressed the need for special internal control systems with respect to modern electronic systems for the modern trends was talk of internal control definition is "an important part of the company's management, which provides reasonable assurance that the following objectives have been achieved: the effectiveness and efficiency of operations. confidence in the financial recognition. compliance with laws and regulations. (Alhosbann & Atallah, 2009, p. 37).

So that internal control systems give way to assess the risks faced by the company, whether internal or external influences. Consistent and clear goals for the company is positioned as a prerequisite for risk assessment, so the risk assessment is to identify and analyze the risks related to and associated with achieving specified in the long-term performance plans goals.

Internal audit was initially designed to search for computational errors in accounting documents and conducting inventory for cash and audit of the financial statements, the auditor did not have full access to all books and records. And the evolution of this concept to scrutiny until the end of 2001 where he appeared last definition is compatible with the following modern concepts: Risk Management. arbitrary actions (institutional). It is a set of rules and methods that prevent corruption or for anyone on the gains are not right. advisory role of the auditor. Thus, the new definition of Internal Auditing issued by the IIA Institute of Internal Auditors (IIA) has become as follows: Activity emphatically independent, objective and advisory designed to enrich and develop the management processes and by helping them to achieve their goals organization in a systematic way to evaluate the effectiveness of risk management and institutional controls and procedures (IIA, 2003, p. 6).

IT audit information: it is based on the use of modern technologies in the field of audit to be used as a tool for auditing, as well as the aim of helping facility management to understand the environment in which the company operates for the risks and opportunities that new technologies and their impact on achieving the objectives of the

company to assess and provide the necessary decision-making information in time appropriate (Alhosbann, Atallah, 2009, p. 79).

Because of the increased use of modern technology in the public shareholding companies, especially in recent years, which are primarily designed to increase efficiency and reduce the conditions of uncertainty and achieve efficiency in the completion of operations and achieve the objectives of companies in general, the information technology mitigation of red tape in the company and the delivery of services to customers easily pleased. Created IT radical changes to the regulatory regime in companies in general and in particular the internal control system, such as changing the storage and registration, deportation and extract reporting process, but they contrast also created a risk to be internal control of discovery and find how to deal with or employ them in order to achieve the company's goals The information technology to restructure the data and extract reports addressing ways, and in return, there is the risk facing organizations that adopt information technology, so it has to be monitored well known to control properties that should be applied to them (Robert L., Braun E., 2003, p. 72).

Internal auditors are interested in these days the risks and the risk assessment process more than ever before, and the main reason for this is the possibility of change in the circumstances surrounding the company's technological developments that affect the activities and the nature of the company's work. Known risk from the point of view of internal control as "conditions of uncertainty of occurrence of which have a significant effect on the company's objectives. These risks are measured in the form of redundancy or large probability of occurrence. Is a definite risk of occurrence under the IT environment when: be the company's existing skills do not affect them, calculates the likelihood of occurrence based on a multitude of notes, and regulatory system is weak (Bielke, Sten, 2005, p. 25.).

The process of information technology to identify critical or sensitive data risk assessment (Critical Data) and to identify the persons who have the authority to enter data and information, and is based on the examination of systems integration and stability, and audit documentation and ownership of these systems, and the decline continued work planning, and based on the policies and procedures for evaluating staff and, finally, based on the testing of internal control system. Availability of computers required to audit the information and networks, in order to get the auditors are able to keep up with information technology, they use computers as a tool to audit, and the use of automated systems, and understand the very work of these systems, and understand the environment in which they operate these systems (Russell, Larry, 2003, p. 2).

Characterized the American Institute of Internal Audit between risk analysis and risk assessment through the following: Risk assessment which is a systematic process to evaluate and integrate the provisions of specialists about the possibility of circumstances and events is appropriate. The risks are that the meaning of discrimination and integration specialists provisions provide for the development work Audit analysis risk analysis that provided a list of pre-checker and supported by the Governing. Risks that should be the focus in the process of evaluating and analyzing the risks in the IT environment as identify and assess the risks of assets (whether tangible or intangible assets) and expressed in monetary form. Examples of intangible assets risks computers risk, utilities, documentation and risk, and the risk of people. With regard to the dangers of intangible assets mismatch: the risk of replacing the data and programs, and the risk of not being able to Operating (Ozier, Wil, 1999, p. 14).

The auditor should be adequately educated about the company and its critical business activities before conducting a data center review. The objective of the data center is to align data center activities with the goals of the business while maintaining the security and integrity of critical information and processes. To adequately determine whether or not the client's goal is being achieved, the auditor should perform the following tasks to perform infrastructure information technology: (Lyon, Gordon, 2006).

- Meet with IT management to determine possible areas of concern;
- Review the current IT organization chart;
- Review job descriptions of data center employees;
- Research all operating systems, software applications and data center equipment operating within the data center;
- Review the company's IT policies and procedures;
- Evaluate the company's IT budget and systems planning documentation;
- Review the data center's disaster recovery plan.

An IT audit is different from a financial statement audit. While a financial audit's purpose is to evaluate whether an organization is adhering to standard accounting practices, the purposes of an IT audit are to evaluate the

system's internal control design and effectiveness. This includes, but is not limited to, efficiency and security protocols, development processes, and IT governance or oversight. Installing controls are necessary but not sufficient to provide adequate security. People responsible for security must consider if the controls are installed as intended, if they are effective if any breach in security has occurred and if so, what actions can be done to prevent future breaches. These inquiries must be answered by independent and unbiased observers. These observers are performing the task of information systems auditing. In an Information Systems (IS) environment, an audit is an examination of information systems, their inputs, outputs, and processing. (Rainer, R. Kelly, and Casey G., 2011).

companies, particularly large ones over dependence on the application of e-business environment in every day, in order to manage its business and activities in a manner and time appropriate, and that the result of the rapid change in the technological developments that affect the work of those corporate environment. The supervision process or the continuity of supervision imposed by the information technology in the light of an electronic work environment based on three principles: practices that are the mechanism used in the company's consistent with the policies established by the company, that there is a possibility to determine the speed at which directors or auditors can identify problems related to information technology or electronic work environment, and that the management to identify employees who are authorized to work in the electronic environment and determine what needs to be done from every employee in that environment. (Baccsam, Prashan, 2003, p. 2).

So that IT Auditor plays the big part of company including the applying of workflow instead of using the paper request form, using the application control instead of manual control which is more reliable or implementing the ERP application to facilitate the organization by using only 1 application. According to these, the importance of IT Audit is constantly increased. One of the most important role of the IT Audit is to audit over the critical system in order to support the Financial audit or to support the specific regulations announced. From the above it can be concluded that due to the rapid change in information technology, it is necessary to develop regulatory measures to be effective, Changes to technology and its applications and the transition to e-commerce and the expansion of communication networks, applications, will change the regulatory activities identified and can be applied and how to apply them. As computer hardware developer puts additional responsibilities for data processing on the responsibility of the end user, it is necessary to identify and apply the necessary regulatory procedures.

Review the information technology or information systems auditing, is the study of the control of existing management within the infrastructure of information technology. Determine the evaluation of the evidence that is obtained for a decision on the ability of information systems to maintain the assets, maintaining data integrity, and is working effectively to achieve the goals or objectives of the organization. These reviews may be implemented in conjunction with the audited financial lists process, internal audit, or other form of joint ratification. IT audit is also known as "automatic data processing (ADP)" and "computer audit." Previously it was called electronic data processing (EDP). (Alhosban, Atallah, 2013, p. 112).

So that Internal auditor must understandability technical information relating to the requirements for fast equipment characteristics, It is also important to address the future expansion requirements for each of the elements, the PL and the CPU, and the unity of moving the least of opportunities and tapes, and data communications devices, And printing devices, and other components of the software. he must be the characteristics of the software include Specific accounting software features and functions required from the user's perspective. He also assumes Tags results to determine the interaction with existing hardware and software and the rules associated with the standard requirements Speed and size of the system and issues of conversion. In addition, it is important to determine the requirements for the Documentation on the technical level and the level of the user and the type of training.

In developing our approach for the IT audit risk assessment we incorporated the Control Objectives for Information and related Technology (COBIT) framework as published by the IT Governance Institute. COBIT is a leading IT governance framework and identifies generally understood IT controls. We also utilized guidance from the Institute of Internal Auditors. We developed a data collection tool in Microsoft Excel which includes criteria for ranking risk according to the process maturity of technical COBIT areas, as well as qualitative factors. The COBIT technical areas included: restricted access, change control, computer operations, backup, and recovery. Qualitative factors included: compliance with regulations, public health and safety, past audit findings, auditor judgment, fraud potential, and management request. The evidence gathering and analysis techniques used to meet our audit objectives included, but were not limited to: Interviewing personnel in Technology Services; Ranking the risk of selected IT areas; and Reviewing results with management. (COBIT, IT Governance Institute 2010).

Once the risk of material misstatement has been assessed for major accounts, transaction streams and disclosures, the auditor must develop an audit plan in which he or she documents the audit procedures that, when performed, are expected to reduce audit risk to an acceptably low level. As the auditor is assessing risk and the design and implementation of internal controls, he or she should determine any overall responses to address risks of material misstatement at the financial statement level, and tailor audit plans (that is, audit programs) to be responsive to the identified risks of material misstatement at the relevant assertion level. The application of a “standard” audit program of procedures on all engagements will generally not be responsive to the risks of material misstatement, and is not an appropriate response under the new standards. Auditors should propose known misstatements to management for adjustment. If they are not adjusted, the auditor should be alert to the risk there may be an underlying reason behind the lack of management response, such as might occur if the correction would trigger the violation of a loan covenant or change the direction of an important trend mea (John A. Fogarty, 007).

3. Statistical Results

Examine the results of the field study, specifically the following topics will be discussed: characteristics of the study sample, the members discuss the statistical results from the arithmetic mean and discussion to test hypotheses and test credibility alpha.

3.1 Validity and Reliability

Alpha has been using the test of credibility for the degree of internal coherence in the study sample members and answers that range from 0 to 1, and the minimum based on the findings and recommendations of the study is 60%, and the alpha value as the study sample members answers is 73% which is higher than the minimum, which means there is sincerity and constancy in the study sample members answers to paragraphs of resolution.

3.2 Characteristics of the Study Sample Members

First: personal information

This section contains three variables are age, education, years of experience and job title, and were as follows :

Table 1. Sample according to age

Statement	Frequencies	Percentage
20- less than 30 years	10	%21
30- less than 40 years	13	%28
40- less than 50 years	18	%36
50 years and more	7	%15
Total	48	%100

Notes from table 1 that the sample is suitable for setting within the age categories as noted that 40-5 years is one of the highest categories, followed by 20-30 years and 40 years or more as a percentage, this may indicate a years experience among members of the study sample, either theoretical or practical because there is a relationship between age and years of experience, the greater the age, the more years of experience, which gives an indication of a good degree of credibility Study of high-resolution paragraphs so there is truth in the findings and recommendations emerging from this research

Table 2. Sample according to education

Statement	Frequencies	Percentage
BA	29	%60
Master	12	%26
PHD	7	%14
Total	48	%100

Notes from table 2 that most sample members who hold a Bachelor's degree from the various qualifications as noted that post graduate have good percentage is 40% and this is a positive indicator and gives credibility somewhat to rely on the findings and recommendations of the study and may give a positive indication of the sincerity of the answer and that the paragraphs of the resolution was clear.

Table 3. Sample according to years of experience

Statement	Frequencies	Percentage
Less than 5 years	14	30%
5- less than 10 years	25	52%
10 years and more	9	%18
Total	48	%100

Note from table 3 that most members of the sample of the study experience class 5-less than 10 years and is a good time to judge the hypotheses of the study variables have a positive advantage in her sincerity and constancy study tool

3.3 The Taking of Decision

I have been using a likert Pentagram Design resolution of five options for each paragraph of resolution for the purposes of statistical analysis was made using system encoding options so was given the following symbols

- 1)-Very high degree given by the icon 5;
- 2)-High score given by the code 4;
- 3)-Medium is given by the symbol 3;
- 4)-Low given the symbol 2;
- 5)-Very low degree given by the symbol 1.

So the average premise for accepting or rejecting the hypothesis would be paragraph or the Middle premise 3, obtained by using a collection of icons and divided into a number of options which $(5 + 4 + 3 + 2 + 1)/5$ is equal to 3. So if the Center paragraph or hypothesis that is greater than or equal to the number 3 it means accepting a paragraph or more premise that setting the higher the degree of acceptance and confirmation of the study sample with that variable, and less central paragraph or hypothesis about the number 3 it means that the study sample tend to lack in practice, the greater the difference from the Center premise further confirm the appointed members in the absence of the effect of that variable in the Bank The study sample members.

Discussion of statistical results with hypotheses of the study variables.

First hypotheses: internal auditor can not cope with infrastructure for IT AUDIT.

Table 4. Views the sample paragraphs in the infrastructure for IT AUDIT

number	Description	average	Standard deviation	Rank
1	Meet with IT management to determine possible areas of concern	3.08	0.35	7
2	Research all operating systems, applications data center equipment operating within the data center	2.49	1.06	8
3	The auditor should ask certain questions to better understand the network and its vulnerabilities	4.15	0.549	1
4	the purposes of an IT audit are to evaluate the system's internal control design and effectiveness	3.72	0.843	3
5	An audit to verify that IT management has developed an organizational structure and procedures to ensure a controlled and efficient environment for information processing	2.19	0.586	9
6	IT Auditor help companies save money by finding ways to use IT hardware and software more efficiently and get a better handle on technology assets	3.28	0.834	5
7	Audits can focus on such major IT assets as ERP systems	4.07	0.642	2
8	Information technology infrastructures have continued to grow in size and complexity. Servers, storage area networks (SANs), and network attached storage (NAS)	3.62	0.934	4
9	Without the ability to assess both existing infrastructure and visibility into the SAN, organizations cannot achieve overall object	3.24	1.18	6
Total		3.31		

Notes from table 4 that the study sample members confirm third paragraph at average 4.15 which represents The auditor should ask certain questions to better understand the network and its vulnerabilities and that means auditor have more information about infrastructure about company and can be help auditor to provide suggestion and recommendations to solve any problem in information technology environment, also noted that seventh paragraph is second confirm by sample members at average 4.07 and that paragraph which represents Audits can focus on such major IT assets as ERP systems and that means auditor can advise management to Invest in IT Assets or decrease the size of amount of investment also he can make general point view about efficiency the used of IT asset, and noted that fifth paragraph has lower acceptance of sample members at average 2.19 which represents An audit to verify that IT management has developed an organizational structure and procedures to ensure a controlled and efficient environment for information processing and that may be means auditors can not make self control on organization structure and find extent to comply with regulation of company. also notes that the average premise is 3.31 and is higher than the average premise 3 and this shows that the study sample members reaffirms and accept the alternative hypothesis and reject the null hypotheses.

Second hypotheses: internal auditor can not cope with IT Audit risks.

Table 5. Views the sample paragraphs in IT audit risks

number	Description	average	Standard deviation	Rank
1	Audit risk assessment is a stage in the audit planning process	4.47	0.924	1
2	Risk assessment provides a mechanism for identifying which risks represent opportunities and which represent potential pitfalls	3.29	0.816	5
3	A good assessment is anchored in the organization's defined risk appetite and tolerance, and provides a basis for determining risk responses	3.09	0.592	6
4	Audit risk assessment Evaluation of risks related to the value drivers of the organization, covering strategic, financial, operational, and compliance objectives	4.31	0.643	2
5	Once the risk of material misstatement has been assessed for major accounts, transaction streams and disclosures	2.48	1.24	7
6	Goals of IT audit Risk Assessment and Management : Accurate view on current and near-future IT-related events	3.76	0.742	3
7	risk assessment is the identification and analysis of relevant risks to the achievement of an organization's objectives	2.38	0.559	8
8	IT audit risk assessment we incorporated the Control Objectives for Information and related Technology	3.58	0.752	4
Total		3.42		

Notes from table (5) that the study sample members confirm the first paragraph at average 4.47 which represents Audit risk assessment is a stage in the audit planning process and that mean auditor make audit strategy by prepare good audit program to avoid risks which affected in performing goals for company and auditors cope with advances with IT tools, and notes the fourth paragraph has second acceptable from sample members at average 4.31 which represents Audit risk assessment Evaluation of risks related to the value drivers of the organization, covering strategic, financial, operational, and compliance objectives and that mean auditors make assurance effective internal control for company and help in making consultation tasks to management whether financial or non financial transaction, and notes the sixth paragraph has third acceptable by sample members at average 3.76 which represents Goals of IT audit Risk Assessment and Management: Accurate view on current and near-future IT-related events and that means it auditors help management in risk assessment and risk specification which can affected in achieved overall objectives for company and can make competitive advantages or make core competences for employees in company which attractive IT tools. also notes that the average premise is 3.42 and is higher than the average premise 3 and this shows that the study sample members reaffirms and accept the alternative hypothesis and reject

3.4 Testing Hypotheses of the Study

First hypothesis That internal auditor can not cope with infrastructure for IT AUDIT. By using the T-test for one sample One Way this t-test to the first hypothesis, the test results according to the following table:

Table 6. The first hypothesis test results

The calculated T	Schedule T	T	statistical	As a result the null	Arithmetic mean
		significance		hypothesis	
7.91	1.977	0		Reject	3.31

Notes from table 6 so that the decision is to accept the hypothesis of nihilism (H0) if the value of the indexed value, and rejects the nihilistic hypothesis (H0) if the calculated value is greater than the value table. So we reject the hypothesis of nihilism and accept the alternative hypothesis that internal auditor can cope with infrastructure for IT Audit

Second hypothesis: That internal auditor can not cope with IT Audit risks. By using the T-test for one sample One Way this t-test to the first hypothesis, the test results according to the following table:

Table 7. The second hypothesis test results

The calculated T	Schedule T	T	statistical	As a result the null	Arithmetic mean
		significance		hypothesis	
7.91	1.977	0		Reject	3.42

Notes from table 7 so that the decision is to accept the hypothesis of nihilism (H0) if the value of the indexed value, and rejects the nihilistic hypothesis (H0) if the calculated value is greater than the value table. So we reject the hypothesis of nihilism and accept the alternative hypothesis internal auditor can cope with IT Audit risks

4. Results and Recommendations

4.1 First Results

- 1)-The auditor should ask certain questions to better understand the network and its vulnerabilities.
- 2)-Audits can focus on such major IT assets as ERP systems and help management to make rational decisions in investing in IT assets to attractive new customers and make core competences for company.
- 3)-the purposes of an IT audit are to evaluate the system's internal control design and effectiveness and its role to compliance with rules and regulation of company.
- 4)-Information technology infrastructures have continued to grow in size and complexity. Servers, storage area networks (SANs), and network attached storage (NAS).
- 5)-Audit risk assessment is a stage in the audit planning process and that mean auditor make audit strategy by prepare good audit program to avoid risks which affected in performing goals for company and auditors cope with advances with IT tools.
- 6)-Audit risk assessment Evaluation of risks related to the value drivers of the organization, covering strategic, financial, operational, and compliance objectives.
- 7)-Goals of IT audit Risk Assessment and Management: Accurate view on current and near-future IT-related events and that means it auditors help management in risk assessment and risk specification which can affected in achieved overall objectives for company and can make competitive advantages or make core competences for employees in company which attractive IT tools.

4.2 Recommendations

- 1)-important to care an audit to verify that IT management has developed an organizational structure and procedures to ensure a controlled and efficient environment for information process.
- 2)-important to care Meet with IT management to determine possible areas of concern.
- 3)-the ability to assess both existing infrastructure and visibility into the SAN, organizations cannot achieve overall object.
- 4)-important to care risk assessment is the identification and analysis of relevant risks to the achievement of an organization's objectives.
- 5)-The need to identify IT risks and how to deal with it through the mitigation of the impact on the overall goals

of the banks.

6)-make conferences and other articles to appear importance of using IT tools and it role in accomplishment core objectives.

References

- Alhosban, A. (2013). Accounting information system.
- Alhosbann, A. (2009). *Internal Audit and Control in the IT environment*. Amman, Jordan
- Alotaibey. (2014). Assess the level of governance of information technology in Taif University using Koepf scale.
- Baccsam, P. (2003). Continuous Monitoring of Application RiskIIA.
- Bielke, S. (2005). Risk Assessment – Mission Impossible.
- COBIT. (2010). IT Governance Institute.
- Janvrin. (2009). An Investigation of Factors Influencing the Use of Computer-Related Audit Procedures. *Journal of Information Systems*, 23(1).
- John, A. F. (2007). Assessing and Responding to Risks in a Financial Statement Audit. *Journal of Accountancy*.
- Kareema, A. J. (2010). The Risk Impact of the Use of Technology in the Job Quality of External Auditors Field Study in Some of the Jordanian Auditing Offices. *Zarqa Journal*.
- Ozier, W. (1999). A Framework for an Automated Risk Assessment tool. *IIA*, 2, 14.
- Rainer, R. K., & Casey, G. C. (2011). *Introduction to information systems* (3rd ed.). Hoboken, N.J.: Wiley.
- Robert, L., & Braun, E. (2003). ComputerAssisted Audit Tools and Techniques Analysis and Perspectives. *Managerial Auditing Journal*, 18(9).
- Russell, L. (2003). CPA have Right to Perform IT Risk Assessment for Clients.

Copyrights

Copyright for this article is retained by the author(s), with first publication rights granted to the journal.

This is an open-access article distributed under the terms and conditions of the Creative Commons Attribution license (<http://creativecommons.org/licenses/by/3.0/>).