International Journal of Economics and Finance; Vol. 7, No. 11; 2015
ISSN 1916-971X E-ISSN 1916-9728
Published by Canadian Center of Science and Education

The Role of the Auditor in Planning and Reduce the Risk of IT Environment in Commercial Jordanian Banks

Mohammed Naser Hamdan[1] & Atallah Hosban[2]

[1] Al Albeit University, Jordan

[2] Irbid National University, Jordan

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

Received: December 29, 2014 Accepted: August 21, 2015 Online Published: October 25, 2015

doi:10.5539/ijef.v7n11p222 URL: http://dx.doi.org/10.5539/ijef.v7n11p222

Abstract

This study aimed to identify the role of the auditor's judgment in dealing with the risks of the IT environment, so I studied the process of IT risk planning , and study how the auditor to reduce the risk of information technology. The study on designing a questionnaire covering the variables and hypotheses of the study , the questionnaire consists of 14 paragraphs, were used methods of statistics such as averages and standard deviations, and percentages and frequencies , and the study sample consisted of auditors (52) (external Auditors)for commercial banks in Jordan , most results are: Auditor determine the output of the likelihood of recurrence of the threat event (incidence of threat), and is expressed in a year ,Auditor Identify risks that cause weakness and imbalance core activities of the company, and monetary loss resulting from it , and Auditor prepare Prioritize risks according to their importance. Study recommendations are: its important to care that the members of the team in charge of identifying risks with a statement of clarification and details in favor of it, based on the knowledge that they own about those risks. And Auditor evaluate on an ongoing basis and on a periodic basis, and this determines the important information should be focused information security on them

Keywords: information technology, planning, risks, commercial banks

1. Preface

Consistent and clear goals for the company put a prerequisite for risk assessment. It intended to determine the risk assessment and analysis of the relationship of risk associated with the achievement of specific performance plans in strategic goals. In determining these risks are analyzed to identify the impact in the application of information technology, because technology punctuated by constant changes as the company's circumstances, so it is necessary to establish clear mechanisms to identify these risks resulting from these changes and how to deal with it. Find information technology activities and large operations, which increased the importance of auditing and control as to increase business deals led to the existence of risk is the inability of the auditor to audit all operations and this in turn requires increased training of personnel in general and workers in particular internal control.

1.1 The Problem of the Study

This study attempts to answer the following questions:

1). What is the role of the auditor in dealing with the risks of information technology in the commercial banks of Jordan ?
2). What is the role of the auditor in mitigating the risk of information technology in the commercial banks of Jordan?

1.2 The Importance of Studying

The information technology risk is based on the restructuring of 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 to identify good control properties that should be applied on them. The internal control and risk attaches' importance to the risk assessment process, and the main reason for this is the possibility of changing the circumstances surrounding the company's technological developments that affect the activities and the nature of the company's business. Because the risks reflect conditions of uncertainty of occurrence of them have a noticeable impact on the

company's objectives. These risks are measured format repetition or large probability of occurrence.

1.3 Hypotheses of the Study

1). No-checker in the planning of the risks of information technology in commercial Jordanian banks;

2). There is no role for the auditor to the alleviation of information technology in the Jordanian commercial banks risk?

1.4 Objectives of the Study

1-To identify the risks of information technology and the role of the auditor in dealing with the effects of those risks;

2-Identify the nature of the risks faced by the auditor in commercial banks, and show the role of the auditor in dealing with the analysis and identification of risks related to information technology;

3-Stated at some of the measures undertaken by the auditor to reduce the risk of information technology.

1.5 The Study Methodology

This study is based on inductive and deductive approach, so that represents inductive approach to books and scientific references and previous studies which will help to cover the theoretical framework of the study, also it represents a deductive approach to design a questionnaire containing variables and hypotheses of the study to get the results and recommendations of the study.

1.6 Society and the Study Sample

The study population consisted of external auditors to commercial banks so that found the number 97 external auditor, questionnaires were distributed to the study sample was randomly so that the distribution of a questionnaire 64 was 52 recovery and identification of the recovery rate 81%.

1.7 Previous Studies

1). Jamran study (2015), "The impact of Using Information Technology in Improving State Budget of Kuwait"

This study aimed to identify the impact of using information technology in the general budget components, and identify the risks and benefits of the using information technology tools in the preparation of the general budget in the State of Kuwait, and the study sample consisted of (89) individuals in the accounting departments in the Ministry of Finance in Kuwait, in addition to the auditors working in the State Audit Bureau of Kuwait. To achieve these goals, the researcher designed a questionnaire consisted of (33) items.

The results showed an impact of using computers and accessories technology in improving the preparation of the general budget in Kuwait, and the results also showed an impact of using software to improve the preparation of the general budget in the State of Kuwait, the results also showed a an impact of using networks communications to improve the preparation of the general budget in the state Kuwait, and finally, the results showed the a role of the training courses for the human element in improving the preparation of the general budget in Kuwait.

The researcher presented a number of recommendations including the need to develop computers for the administration to improve the efficiency of public expenditure and revenue which requires to reduce the budget deficit, and the need to apply the latest management for the preparation of the general budget of the training programs

2). Alhosban study (2014), "Impact of conditional factors on internal control system in keeping with the requirements of information technology from the point of view of IT auditors at commercial banks in Jordan"

This study aims to Identify the linking of police supervision of the internal control system and identify the impact of these link in promoting the concept of banking supervision, and highlight the concept of conditional and control areas of evolution and their use. this study depends up on deductive approach: through the questionnaire user-friendly design and characteristics of the study include the study variables and assumptions. the most finding of this study: An Auditors provide management about the reliability of it systems and how to control environmental factors both internal factors or external factors and internal oversight helps to identify opportunities and threats of the external environment and identify the strengths and weaknesses of the internal environment factors, An Auditor shall determine the conditions of uncertainty in the information technology environment which reduces risks of modern technology and investment opportunities by internal oversight , and Auditors should focus on expanding the information and try to adjust its deployment in large organizations because it will have a wide range of information about internal activities. and main recommendation are: The auditor training and education programmers on information security risks and their impact on the company's

working environment, The role of internal audit and the internal control system in determining a company's information technology tools, audit, and determine the costs for those programs, and Conferences, seminars, known researcher conditional control factors on large business organizations particularly banks

3). Abu-Musa (2008), "Information technology and its auditing: An empirical study of Saudi implications for internal Organization"

The study aimed to demonstrate the impacts of information technology on internal auditors' activities, where the study sample consisted of (700) Checker auditors were selected from organizations working in Saudi Arabia. It was the use of statistical methods such as multiple regression and financial ratios and results of the study showed that internal auditors need to enhance their knowledge and skills in computerized accounting information systems to be used for the purposes of planning, direction, supervision and reporting and corporate budgets. The results showed that internal auditors link to information technology entail several factors: to clarify the goal of the audit, and knowledge of the type of industry, and assess the necessary number Information Technology Audit. The study recommended the need to train auditors on the latest IT technologies.

1.7.1 The Present Study Different from Previous Studies

1-It is based on knowledge of the measures which the auditor must be done to plan for proper risk IT;

2-Can specify actions to be taken into account to deal with the risks of the IT environment;

3-That is based on the linking information technology with the work of the internal auditor in the commercial environment Jordanian banks planning process.

2. The Theoretical Framework of the Study

It characterized the American Institute of Internal Audit between the risk analysis and risk assessment, through the following: (Alhosban, 2009, p. 95).

1). Risk assessment, a regular process for the assessment and integration of the provisions of the specialists about the possibility of circumstances and events is appropriate.

2). The risk analysis are that the meaning and discrimination and the integration of the provisions of the availability of specialists to develop the work audit risk analysis that list supplied by the auditor-backed administration must pass the following stages.

First, analysis and risk assessment.

Second, the analysis of the probability of loss of cash resulting from the risks and effects caused by them.

Third, use the same software used in other companies in order to take advantage of the possible benefits obtained, such as: reducing the cost of the programs, and application development and maintenance, and support from other users, and easily the presence of staff.

For the integration of auditors and the efforts of workers in the field of internal control to identify the risk and assess the relative importance of its levels, it would require an effective way to follow in assessing those risks, because the ability to determine the degree of risk and the level of impact on the audit procedures. And the best ways to analyze and assess the risk is to follow the analytical procedures (Analytical Procedures), which helps to shorten the time, adding to it a preferred method to accomplish and understand the wishes and requests of customers. (Silton, 2004, p. 4).

So that, 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 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 evaluation staff and, finally, based on the testing of internal control system.

The most important audit in general and internal control, particularly in the information technology work environment, is to identify high on the Organization dangerous sites, The auditor should participate with management in the risk assessment process, to ensure the views stability around those risks to be interesting management and auditors in evaluation of priorities risk analysis so start first analyzed the risk of the auditor, and then assess the likelihood of exposure and finally determine the costs of those risks (Grand, 2003, p. 6).

Auditors specialists in the audit of information technology should pay attention to risk management and understand the cost-benefit analysis, because companies generally possess valuable information consists of: customer files, and the Strategic Plan, and budgets, so must the auditor assist management in determining when information security appropriate, and It must be managed, in order to prevent leakage of such information

(Lawrence, 2004, p. 14).

2.1 Special Rules in the Measurement of Risk Assessment Planning in Light of the Information Technology Environment from the Point of View of Auditor: (Jacobson, 2002, p. 8).

1) Identify risks that cause weakness and imbalance core activities of the company, and monetary loss resulting from it.
2) Determine the possibility of a loss (loss of appropriate risk), including special functions and those related to risk assets, preferably expressed in monetary form.
3) Determining the monetary amount of the loss or weakness resulting, from the occurrence of the threat (and this related to the second point).
4) Determining the output of the likelihood of recurrence of the threat event (incidence of threat), and is expressed in a year
5) Determining the possibility of dealing with the major issues of the gravity: conditions of uncertainty. And how to determine the circumstances, and what to do if you are.
6) Determine the cost efficiency of using either the rate of return on investment or use of cost-benefit.

So that The information technology risk, whether it be for information or the infrastructure of the company, the organizations assess the risks of new technology based on the basis of those risks and their relationship with the company, such as: application performance, and the delivery systems information, security, and scalability gradient or corrosion (vulnerability).

Definite risk of occurrence in the light of the information technology environment when: be the company's existing skills do not affect them, calculated the probability of occurrence based on a multitude of notes. And be weak regulatory system (Prashan, 2003, p. 8).

So that Provide computer hardware and networks required to auditing the information, 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 work of these systems, and understand the environment in which they operate these systems.

2.2 The Steps to Be Carried out from the Viewpoint of the Auditor to Reduce the Information Technology Risk Assessment Information Technology Risk: (Randy, 2002, p. 13)

1) Identify information assets: The mission must determine the assets of each circle, and these task assets include: computer parts, software, and systems, and related services, as well as related technology.
2) To compile and prioritize those assets: After you have completed the first step, the second step is an order of assets according to their importance, whether very sensitive so you can not carry out any action without or non-sensitive, while the second arrangement is suitable information can be dispensed with for several days and no longer than a week, while the third place and the last of the information they are regular information that can be dispensed with and can get the job done without activities for a long time
3) Risk identification: Here identify all risks circle whether these problems or specific or non-specific threats. And the risks should be concrete and specific to one or more of the assets.
4) Prioritize risks according to their importance: These circles give an idea of the places of events that need to be planning; it is also working on the development of sequential steps, making the process more easily managed. So that it is sensitive in the highest priority risk status
5) Develop a list of risks: Here are the members of the team in charge of identifying risks with a statement of clarification and details in favor of it, based on the knowledge that they own about those risks.
6) Work appropriate recommendations to find solutions to these risks: In this step the working group to draw up a list of sensitive assets (the most vulnerable) sorted by priority in a separate part of the risk assessment report. This helps departments to propose appropriate solutions to those risks and the implementation of plans to protect those assets.

2.3 Risk Analysis Planning Report Components: (Randy, 2002, p. 15)

1) Title of the paper: contains the name of the department and the names of the working group in charge of risk assessment planning.
2) General Information: Refers to the department manager, team leader, and the dates of the analysis.

3) Concerns (public proposals): care proposals constituency concerned.

4) Asset Information: put sensitive assets by each department priorities.

5) Establish priorities for risk: the risk exposure in order of importance with the proper definition of these risks.

6) Recommendation: identify known option to describe the risks by cost method, or yield.

There are skills to be of its existence so that it can help employees and customers of information security risk management and prevent them from legal accountabilities caused by viruses or abuse, or any other breaches of security that tools and procedures routine play an important role in ensuring that unauthorized access by individuals information stored on the computer, the human behavior plays a strong and effective role in information security procedures by setting passwords and security measures to make sure the information entrusted to him (Scott , 2003, p. 4).

It must be principles, standards and norms and the mechanism of coordinated and integrated security information among them and are integrated with policies and procedures relating to the maintenance of information security through information systems in the company. Because some breaches of information security may be the result of lack of control, so the information security must be appropriate when more planned and coordinated through control systems in the company and through the life of that information (Grand, 2000, p. 6).

It must be assess the risk of information systems in and information and requirements for information security differ succession periods on the company, and the information, whether in terms of the probability of occurrence or recurrence must be evaluated on an ongoing basis and on a periodic basis, and this determines the important information should be focused information security on them, from those that did not become a form of great importance for the company, and therefore the possibility of identifying the risks or mitigate the effect of interest that are information security cost appropriate and reasonable (Grand, 2000, p. 6).

3. Statistical Analysis

After the completion of the theoretical framework of the subject of the study, and after the distribution of the questionnaire to a sample study, the introduction of the questionnaire data on statistical analysis program was used the following tests: Test Alpha stability and credibility, one sample T Test, percentages and standard deviations, and the arithmetic average .

3.1 The Credibility of the Study Tool

We found the value of alpha test-the degree of internal consistency of the answers the study sample-The Cronbach's alpha test the value of 79%, a statistically acceptable to rely on the findings and recommendations of the study ratio, where the minimum value of the alpha statistically acceptable 60%. Therefore, the degree of internal consistency of the answers the study sample a good percentage of the adoption of the validity and reliability of study tool.

3.2 Base Decision-Making

Been using a system of Likert Quintet in design resolution, so were given weights of each resolution options, so that was given weight 1 is strongly non OK, and weight 2 to non-OK, and weight 3 to neutral, and weight 4 to OK and weight 5 strongly OK, so the central premise is 3, whenever central premise is greater than 3, it means that the study sample have agree of approval of the resolution paragraph, while central premise is less than 3, it means that the study sample have disagree of approval of the resolution paragraph .

3.3 Description Study Sample

Table 1. Characteristics of the study sample according to specialization

Title	Frequencies	percentage
Accounting	42	80%
Financial	5	10%
Management	3	6%
Economics	2	4%
Total	52	100%

Notes from Table 1 that the majority of the study sample who hold specialty accounting, and this may be normal because the accounts of the most important conditions Checker that have obtained a specialization accounting

auditor , and this is a positive sign to believe the study tool for the paragraphs of the questionnaire studied from people who are familiar with the theory of accounting matter which helps to understand the clauses and a positive reflection on the findings and recommendations of the study.

Table 2. Characteristics of the study sample according to year's experience

Title	Frequencies	percentage
Less than 6 years	14	27%
6-less than 12 years	17	33%
12-less than 18 years	12	23%
18 years and more	9	17%
Total	52	100%

Notes from Table 2 that the study sample them almost ratios are similar in years of experience, with a note that the 6-12 years category represent the highest proportion, and this shows the sample members study are suitable for specific expertise in the area of dealing in auditing commercial banks, and this is the index positively to the findings and recommendations of the study.

3.4 Discuss the Results with Statistical Variables of the Study

Table 3. Opinions sample variable information technology planning

Number	Paragraph	Average	Standards deviation	Rank
1	identify the persons who have the authority to enter data and information, and based on the examination of systems integration and stability	3.18	0.425	4
2	The auditor should participate with management in the risk assessment process, to ensure the views stability around those risks to be interesting management	4.57	0.383	1
3	Auditors specialists in the audit of information technology should pay attention to risk management and understand the cost-benefit analysis	2.19	0.46	7
4	Auditor Identify risks that cause weakness and imbalance core activities of the company, and monetary loss resulting from it	3.38	0.749	3
5	Auditor determine the output of the likelihood of recurrence of the threat event (incidence of threat), and is expressed in a year	4.23	0.63	2
6	Provide computer hardware and networks required to auditing the information, in order to get the auditors are able to keep up with information technology	3.09	0.85	5
7	Auditor use of automated systems, and understand the work of these systems, and understand the environment in which they operate these systems	2.42	0.96	6
average		3.37		

Notes from Table 3 that the study sample confirms that the second paragraph is the greatest degree of acceptance at an average 4.57, and this shows that the largest proportions of non-corresponding approval rates, and represented by this paragraph The auditor should participate with management in the risk assessment process, to ensure the views stability around those risks to be interesting management, This shows that the planning for the risk of IT process starts from cooperation auditor and members of the management company, which helps to exchange ideas in dealing with information technology tools and reduce risk of effects on the Bank, also notes that the fifth paragraph represents the second degree of acceptance in the opinion of the study sample average of 4.23, higher than the central premise of this paragraph and represented Auditor determine the output of the likelihood of recurrence of the threat event (incidence of threat), and is expressed in a year, This shows that the internal auditor is the process of planning for the expected risk over a given period resulting from the use of information technology as tools based on the possibility of expression in monetary terms or financial effect on the financial statements, which means the existence of prior planning about potential risks and how to deal with it, Also notes that the minimum degree of acceptance in the opinion of the study sample of the third paragraph members average, less than 3 and this shows that members of the sample does not confirm the existence of this paragraph Auditors specialists in the audit of information technology should pay attention to risk management and understand the cost-benefit analysis. Also notes that the average variable is 3.34, higher than the central premise p This indicates that the sample of the study confirms that the variant of the planning tools applied

information technology in the Jordanian commercial banks a good degree.

Table 4. Opinions sample variable reduce information technology risks

Number	Paragraph	Average	Standards deviation	Rank
1	Auditor identify The mission must determine the assets of each circle, and these task assets include: computer parts, software, and systems, and related services, as well as related technology.	3.69	0.48	3
2	Auditor identify all risks circle whether these problems or specific or non-specific threats. And the risks should be concrete and specific to one or more of the assets.	4.35	0.37	2
3	the members of the team in charge of identifying risks with a statement of clarification and details in favor of it, based on the knowledge that they own about those risks.	2.49	0.81	7
4	Auditor prepare Prioritize risks according to their importance	4.67	0.46	1
5	Work appropriate recommendations to find solutions to these risks by Auditors	3.67	0.58	4
6	Auditor assess the risk of information systems in and information and requirements for information security differ succession periods on the company	3.48	0.98	5
7	Auditor evaluate on an ongoing basis and on a periodic basis, and this determines the important information should be focused information security on them	2.61	0.86	6
average		3.58		

Note from Table 4 that sample members approve that fourth paragraph represents first acceptance at average 4.67 ant it more than 3 which represent that auditors prepare Prioritize risks according to their importance it shows that when make priority for risks which related to information technology that positive effect to minimize the risks on banks, also noted that second paragraph have second acceptance according sample members at average 4.35 which represents Auditor identify all risks circle whether these problems or specific or non-specific threats. And the risks should be concrete and specific to one or more of the assets and that means auditors prepare risks specification and its effects on banks , also noted that average for variable as whole is 3.58 and this more than 3 which means that auditor deal with all things minimize the risks in banks .

4. Results and Recommendations

4.1 Results

The study found the following results:

1) The auditor should participate with management in the risk assessment process, to ensure the views stability around those risks to be interesting management;
2) Auditor determine the output of the likelihood of recurrence of the threat event (incidence of threat), and is expressed in a year;
3) Auditor Identify risks that cause weakness and imbalance core activities of the company, and monetary loss resulting from it;
4) Auditor prepare Prioritize risks according to their importance;
5) Auditor identify all risks circle whether these problems or specific or non-specific threats. And the risks should be concrete and specific to one or more of the assets;
6) Auditor identify the mission must determine the assets of each circle, and these task assets include: computer parts, software, and systems, and related services, as well as related technology.

4.2 Recommendations

Based on the results of the study can be made the following recommendations:

1) Its important to care that the members of the team in charge of identifying risks with a statement of clarification and details in favor of it, based on the knowledge that they own about those risks.
2) Auditor evaluate on an ongoing basis and on a periodic basis, and this determines the important information should be focused information security on them.
3) Auditor assess the risk of information systems in and information and requirements for information security differ succession periods on the company.

4) Auditors specialists in the audit of information technology should pay attention to risk management and understand the cost-benefit analysis.

5) Auditor use of automated systems, and understand the work of these systems, and understand the environment in which they operate these systems.

References

Abu-Musa. (2008). Information technology and its auditing: An empirical study of Saudi implications for internal Organization. *Managerial Auditing Journal*. http://dx.doi.org/10.1108/02686900810875280

Alhosban, A. (2009). *Auditing in information technology environment*. Amman, Jordan.

Alhosban, A. (2015). Impact of conditional factors on internal control system in keeping with the requirements of information technology from the point of view of IT auditors at commercial banks in Jordan. *International Journal of Economic and Finance*.

Al-jamran, A. (2015). The impact of Using Information Technology in Improving State Budget of Kuwait (Master Thesis). Al-Bayt University, Mafraq, Jordan.

Grand , C., & Ozier, W. (2000). Information security management element, audit and control. *IIA, 8*.

Grand, C. (2001). Information Technology on Auditing. *IIA*, 2001.

Jacobson, R. (2002). Quantifying IT Risk. *IIA, 5*.

Lawrence, R. (2002). Risky Business Team With Audit Committee To Tackle With IT Security Needs. *Journal of Accountancy*, June, 2002.

Prashan, V. B. (2003). Managing separation of duties using continuous monitoring. *IIA, 6*.

Randy, M. (2002). Seven-Step IT Risk Assessment. *IIA, 5*.

Scott, C. (2003). A CPA Guide to the Top Issues of Technology. *Journal of Accountancy*, May, 2003.

Silton, J. (2003). Using audit tools to audit software asset, audit tolls. *IIA, 6*.

Copyrights