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

Atallah Alhosban

Received: 13 December 2013 Accepted: 2 January 2014 Published: 15 January 2014

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 resultsAudits 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 . 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.

Index terms—

1 Introduction

mong the most common expectations of internal audit is to gain assurance on financial controls, the reliable execution of audit plans, and coordination with the external auditor. But given the lack of specific guidelines or requirements regarding internal audit's responsibilities, there is a broad range of practice based on organizational needs, structure, and culture. Audit committees can play an important role in confirming the whole organization is on the same page regarding the goals for internal audit, and in providing a strong avenue of communication for the chief audit executive to share concerns and perspectives. This issue of the Audit Committee Brief focuses on the evolving role of the internal audit function, and provides considerations for how audit committees can effectively work with management and internal audit to maximize the value of the function in the context of a company's specific circumstances. The audit observed that work was under way to develop an IT strategic plan and an IT infrastructure asset management policy, and to finalize the IT architecture governance model and processes.

Author: e-mail: aalhosban@gmail.com a) Problem of study 1. is internal auditor cope with infrastructure for IT AUDIT? 2. is internal auditor cope with audit risk analysis ? b) Hypotheses of study 1. Internal auditor can not cope with infrastructure for IT AUDIT. 2. Internal auditor can not cope with audit risk analysis.

2 c) Objectives of study

This study achieve following targets 1. The audit objective was 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 2. management activities (internal control practices, methods and procedures) implemented to avoid potential business impacts or change-related incidents associated with developing, implementing or

changing the IT infrastructure 3. analyze risk assessment and know the role of it auditors to deal with risks which threats attain strategic objectives d) Importance of study

The primary functions of an IT audit are to evaluate the systems that are in place to guard an organization's information. Specifically, information technology audits are used to evaluate the organization's ability to protect its information assets and to properly dispense information to authorized parties, so Technological innovation process audit, This audit constructs a risk profile for existing and new projects and The audit will assess the length and depth of the company's experience in its chosen technologies .

The researcher adopted a descriptive analytical study ends, this section deals with the methodology adopted by the study in detail through the following aspects :

The outcomes of these activities should strengthen IT infrastructure planning, IT asset life-cycle management and IT architecture governance.

3 II.

4 Methodology of the Study

First: Data collection methods In this study rely on two sources of data collection 1. Secondary sources: By reference to Arabic and foreign books, journals, articles, periodicals, as well as the studies, and field research, which was in Jordanian society, and specialized scientific conferences and various sites on the Internet for theoretical study 2. Primary sources: Have been collected through the questionnaire prepared by the previous studies and research .

5 Previous studies 1. Study Weidenmier "Opportunities in Information

Technology and Internal Auditing" IT auditors should be "IT-literate" when it comes to assessing the security measures of a firm's computer systems. Many companies use "cookies" and webscripts in order to gain information from users including consumers, employees of the company, etc. IT auditors should be able to configure the network to keep unauthorized access from occurring in the systems. In order to make sure that the computers are secure before or after an audit, the IT auditor should create a firewall; and install anti-virus/anti-malware programs to prevent hijacking and hackers from gaining access causing identity theft and fraud **??**Weidenmier 2006).

Although this journal article was based on a written paper, I believe this source to be reliable for both auditors practicing in the field and students who may be writing a paper. The article comes from a scholarly journal database and all sources and citations are correctly cited in this source. It is also credible because of the number of citations and sources used, which was approximately 4 pages long of references. The source created in 2006, which is only a few years old but is much more reliable than a source created 10 years ago because technology changes drastically each year, if not each day **??**Weidenmier 2006 Provide data on the extent to which computerrelated 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.

6 Study of FOGARTY 2007" Assessing and

Responding to Risks in a Financial Statement Audit " The Auditing Standards Board issued eight standards with new guidance for auditors assessing risks and controls in financial statement audits. Auditors must consider risk and also determine a materiality level for the financial statements taken as a whole. Auditors are required to obtain a sufficient understanding of the entity and its environment, including its internal control, to assess the risk of material misstatement. Auditors must develop audit plans in which they document the audit procedures that are expected to reduce the audit risks to acceptably low levels. To rely on the effectiveness of company internal controls, the auditor should test the controls, but only after assessing that the design is effective. The auditor may rely on control tests and other evidence from prior audits when the audit evidence and related subject matter have not changed. At the end of an audit, the auditor must evaluate whether the financial statements taken as a whole are free of material misstatements. The auditor must accumulate all the known and likely misstatements, other than trivial ones, and communicate them to the appropriate level of management. In assessing deficiencies of internal controls to identify the severity, the auditor should focus on issues such as inadequate documentation and unqualified employees who lack the skills to make the required GAAP accounting computations, accruals or estimates, or to prepare the company financial statements.

7 Study of Janvrin 2009 " An Investigation of Factors

Influencing the Use of Computer-Related Audit Procedures Provide data on the extent to which computerrelated 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 James Bierstaker An Investigation of Factors Influencing the Use of Computer-Related Audit Procedures JOURNAL OF **??**NFORMATION SYSTEMS , vol 23 , 2009 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 : **??**yon, Gordon (2006) 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. Cegielski. Introduction to information systems. 3rd ed. Hoboken, N.J.: Wiley ;, 2011

Goodman & Lawless state that there are three specific systematic approaches to carry out an IT audit : Richard A. Goodman; Richard Arthur Goodman; Michael W. **??**awless (1994). Technology and strategy: conceptual models and diagnostics. Oxford University Press US. ISBN 978-0-19-507949-4. Retrieved May 9, 2010.

1. Information Processing Facilities: An audit to verify that the processing facility is controlled to ensure timely, accurate, and efficient processing of applications under normal and potentially disruptive conditions. 2. Systems Development: An audit to verify that the systems under development meet the objectives of the organization, and to ensure that the systems are developed in accordance with generally accepted standards for systems development. 3. Management of IT and Enterprise Architecture: An audit to verify that IT management has developed an organizational structure and procedures to ensure a controlled and efficient environment for information processing

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.

IT professionals from the help desk to the CIO have been charged with implementing mechanisms both native and third-party to address their enterprise IT auditing needs. This task up close appears daunting to many and with good reason. The enterprise of today operates 24x7x365 and is subject to stresses of access and modifications invoked by hundred and sometimes hundreds of thousands of people each day. This growing need to audit the enterprise should come as no surprise to anyone who has been in an IT role for the past 5-10 years. Knowing who changed what, when and where throughout the organization can save hours of troubleshooting, satisfy compliance needs, better secure the environment and permit administrators to manage multiple resources that frequently outnumber staff that are now at the critical core of operations. What's most challenging is the diversity of platforms, systems and tools employed over the years just to sustain these daily operations. Now, various regulatory entities combined with a heightened awareness on IT security, the demands presented by auditing all of these systems around the clock in all corners of the enterprise may seem as though it were a perfect storm. Netwrix Corporation, How to Effectively Audit Your IT **??**nfrastructure, 2008) IT audits not only reveal weaknesses in compliance, security, and other areas but also help companies save money by finding ways to use IT hardware and software more efficiently and get a better handle on technology assets. Organizations can use IT audits to ensure that their technology initiatives are in sync with business goals and practices. There are many types of IT audits that cover a broad range of technologies and processes. One type assesses IT governance, determining how well the IT department is managed and staffed, and how efficiently it supports business operations. Information-security audits examine security policies and such technologies as firewalls, as well as analyze the integrity of networks, databases, operating systems, Web servers, and applications. Audits can focus on such major IT assets as ERP systems or on individual applications like payroll and accounts payable. Some audits evaluate the effectiveness of business-continuity and disasterrecovery programs, and others make sure that organizations have adequate and up-to-date software licensing in place Adding to this challenge are IT operations that are required to function on tight budgets under constant watch even more so than revenuegenerating functions of an organization. Leaders

keep asking for more while tightening budgets and the only way to successfully secure, manage and maintain the infrastructure is to implement enterprise-wide IT auditing. Bob Violino, CFO IT , Audit Your Technology **??**nfrastructure , 2004) Information technology infrastructures have continued to grow in size and complexity. Servers, storage area networks (SANs), and network attached storage (NAS) landscapes have grown exponentially over time into both larger physical and virtual footprints. With the increase of size and complexity of virtualized server, storage and network infrastructures, organizations are often unable to collect data on their environments and compare it to best practices. As a result, organizations are challenged to identify how to optimize their IT operations. SANs are the backbone for the rapid, uninhibited delivery of data to applications. That means continuous SAN availability is a critical requirement for business success in many market segments. SANs are also becoming increasingly complex, virtualized, MultiFinder environments with embedded services. Without the ability to assess both existing infrastructure and visibility into the SAN, organizations cannot achieve overall objectives. Top objectives include reducing costs, improving efficiency, and becoming more flexible and aligned to their business.

Baccasam, V.Plasham, ”Continuous Monitoring of Application Risk ”,IIA, Vol .6 , May 15, 2003.

Audit risk assessment is a stage in the audit planning process. During the assessment, an auditor determines the likelihood of audit risk, defined as the possibility of recording an inappropriate opinion on an audit as a result of a misstatement in the financial documents examined. Audit risk assessment is part of the series of controls which are used to manage the integrity of an audit, and to determine when and how audits should be conducted, and by whom. Audit risk consists of several components. The first is the likelihood that a material misstatement will be made in financial documents. The second is the risk that the misstatement will not be caught by internal controls, and the third is that the misstatement will not be caught by an auditor. These components are examined during an audit risk assessment to come up with a numerical score which can be used to make decisions about the auditing process. (Alhosban, Atallah, Auding and internal control in information technology invironment, dar alhamed , 2009 , p 96)

Risk assessment provides a mechanism for identifying which risks represent opportunities and which represent potential pitfalls. Done right, a risk assessment gives organizations a clear view of variables to which they may be exposed, whether internal or external, retrospective or forward-looking. A good assessment is anchored in the organization’s defined risk appetite and tolerance, and provides a basis for determining risk responses. A robust risk assessment process, applied consistently throughout the organization, empowers management to better identify, evaluate, and exploit the right risks for their business, all while maintaining the appropriate controls to ensure effective and efficient operations and regulatory compliance. Ozier , Will ,” Information Security Risk Education and Awareness”, Risk **??**anagement , Vol. 6 , July 15, 2003. Audit risk assessment Evaluation of risks related to the value drivers of the organization, covering strategic, financial, operational, and compliance objectives. The assessment considers the impact of risks to shareholder value as a basis to define the audit plan and monitor key risks. This top-down approach enables the coverage of internal audit activities to be driven by issues that directly impact shareholder and customer value, with clear and explicit linkage to strategic drivers for the organization Information technology risk assessment. Evaluation of potential for technology system failures and the organization’s return on information technology investments. This assessment would consider such factors as processing capacity, access control, data protection, and cyber crime. This is typically performed by an organization’s information technology risk and governance specialists. (Jacobson, Robert, ”Quantifying IT Risk” , IIA, Vol. 5 , **??**ugust 15 , 2002) Overall responses to address the assessed risks of material misstatement at the financial statement level may include emphasizing to the audit team the need to maintain professional skepticism. assigning more experienced staff or those with specialized skills or using specialists. providing more supervision. incorporating additional elements of unpredictability in the selection of further audit procedures to be performed. making general changes to the nature, timing, or extent of audit procedures . The assessment of the risks of material misstatement at the financial statement level and, thereby, the auditor’s overall responses are affected by the auditor’s understanding of the control environment. An effective control environment may allow the auditor to have more confidence in internal control and the reliability of audit evidence generated internally within the entity and, thus, for example, allow the auditor to conduct some audit procedures at an interim date rather than at the periodend. Deficiencies in the control environment, however, have the opposite effect (for example, the auditor may respond to an ineffective control environment (SAS No. 122 , Performing Audit Procedures in Response to Assessed Risks , December 15, 2012)

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 , Assessing and Responding to Risks in a Financial Statement Audit , Journal of accountancy , 2007)

Auditors are expected to gain an understanding of client systems and business processes by examining (1) significant transactions supporting the client's financial statements, (2) procedures used to initiate, record, process, and report transactions, (3) means by which client's systems capture events and conditions (other than transactions), and (4) processes used to prepare client financial statements Auditors are also encouraged to review automated controls. Given the importance of these controls, auditors need to determine if these controls are functioning as intended and are continuing to operate effectively. Automated controls include both application and general controls (e.g., program change controls, access controls, and systems software controls). The new audit risk standards (AICPA 2006) expand upon several SAS No. 94 concepts. For instance, the standard on audit evidence suggests that auditors employ computerassisted audit techniques (CAATs) to check the accuracy of the summarization of a file or to re-perform procedures (i.e., aging of accounts receivable, etc.; **??**ICPA 2006, AU 308.33-34)

8 New York, NY: AIC

There may be certain circumstances (i.e., significant client IT-related risks and/ or limited auditor IT expertise) in which it is necessary to use an IT specialist . For instance, as suggested by the planning and supervision standard, auditors may elect to use IT specialists to perform the following procedures: (1) inquiry of client IT personnel about how transactions are initiated, recorded, processed, and reported, and how IT controls are designed, (2) inspect systems documentation, (3) observe the operation of IT controls, and (4) plan and perform tests of IT controls . Hunton, J. E., **??**. Wright, and S. Wright. 2004. Are financial auditors overconfident in their ability to assess risks associated with enterprise resource planning systems? Journal of Information Systems 18 (Fall): 7-29.

Throughout the audit fieldwork, the audit team observed several instances where controls are properly designed and being applied effectively for IT infrastructure, as reflected in the strengths listed below: A list of standards for selected IT hardware, software, and network infrastructure is posted on the PCH intranet site, and maintained by the IT Service Desk, Procurement of IT infrastructure by Sectors/Branches that is not included in business plans is reviewed for consistency with PCH standards by the CIO Branch prior to approval by Contracting and Materiel Management Directorate (CMMD)., ,Business cases prepared for IT projects proposed in integrated business plans consider common or shared IT services where appropriate , On-going monitoring of critical PCH IT infrastructure is performed, and monthly reports are provided on results related to infrastructure availability, such as storage capacity, bandwidth usage, and the response of the service desk to logged incidents , and IT service desk technology is effectively used to manage IT infrastructure-related service desk calls, and to produce detailed reports on service call trends. Majesty Goals of IT audit Risk Assessment and Management : Accurate view on current and near-future IT-related events, End-to-end guidance on how to manage IT-related risks, Understanding of how to capitalize on the investment made in an IT internal control system already in place Integration with the overall risk and compliance structures within the enterprise Common language to help manage the relationships, and Promotion of risk ownership throughout the organization Complete risk profile to better understand risk . Assessing & Managing IT Risk, ISACA Pittsburgh Chapter Meeting October 18, 2010, p7

Risk assessment is the identification and analysis of relevant risks to the achievement of an organization's objectives, for the purpose of determining how those risks should be managed. Risk assessment implies an initial determination of operating objectives, then a systematic identification of those things that could prevent each objective from being attained. In other words, it's an analysis of what could go wrong. Not all risks are equal. Some are more likely than others to occur, and some will have a greater impact than others if they occur. So, once risks are identified, their probability and significance must be assessed., alhosban.

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.

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 .

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.

First: personal information This section contains three variables are age, education, years of experience and job title, and were as follows : Notes from table no. (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. 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.

9 Statistical Analysis

V.

Validity and Reliability VI. 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 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.

10 Characteristics of the Study Sample Members

First hypotheses: internal auditor can not cope with infrastructure for IT AUDIT **??**) 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 nsuggestion 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 loer aceeptance 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

11 Year ( )

A 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 **??**) 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.

12 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: 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 internal auditor can cope with IT Audit risks.

X.

13 Results and Recommendations

14 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 it 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 nearfuture 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.

Second: 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. Make conferences and other articles to appear importance of using IT tools and it role in accomplishment core objectives for company. [1] [2]

SecTools.org. Retrieved 2006-08-24.

? 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.

The auditor should ask certain questions to better understand the network and its vulnerabilities. The auditor should first assess what the extent of the network is and how it is structured. A network diagram can assist the auditor in this process. The next question an auditor should ask is what critical information this network must protect. wikipedia, Information security audit 2009 , auditing information security.

Figure 1:

Figure 2:

1

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

Figure 3: Table 1 :

2

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

Figure 4: Table 2 :

3

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

Figure 5: Table 3 :

4

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, software applicationsdata 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 (

Figure 6: Table 4 :

5

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 (

Figure 7: Table 5 :

5

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

Figure 8: Table 5 :

6

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

Figure 9: Table 6 :

[1]© 2014 Global Journals Inc. (US)
[2]© 2014 Global Journals Inc. (US) 1