J. Glob. Innov. Agric. Soc. Sci., 2016, x(x): xxx.
ISSN (Online): 2311-3839; ISSN (Print): 2312-5225
DOI: xxx
http://www.jgiass.com

EVALUATION OF IT AUDITS IN LOCAL FRAMEWORK

Madeeha Kareem* **and Nafees Ayub**
Department Computer Science and Information Studies
GC University, Faisalabad

*Corresponding author' s e-mail: madihach89@yahoo.com

The main emphasis of this study is to present the efficient method of auditing for numerous information systems (IS) entities that save considerable resources of an organization that is cost, time and efforts. Technologies and expertise has boosted up the data shearing and processing which has substantial influence on controlled environment. Audit technology or audit information system is the analysis of control management within Information technology (IT) infrastructure. As the information systems are protection properties, maintenance of data reliability and effective operational process attain the objectives of establishment. "Automated data process (ADP) audit" and "computer audit" are also known as information technology (IT) audit, formally named "electronica data processing audit (EDP)". Information technology IT audit includes two phases. In initial phase involves the planning and collection of data while in final phase the execution inside controlled structure. IT audits asses the system in place to protect the information of establishment. Capacity of an organization was asses by the IT audits and safe the information, moreover distribute the sharing of data to sanctioned parties. In this study suggested goals compared with different audit frame works and provided the strategies to manage these risks utilizing a unique automated method that can save considerable resources (time, cost and effort) of organization.

Keywords: IT audit, Electronic data processing (EDP), automated data processing (ADP), audit techniques.

INTRODUCTION

Information technology audit is the progression of assessing that the designed computer system had ability to maintain the data, protection of data, effective goal approaches and user friendly environment. The operative information system has the ability to accomplish goals efficiently by using least resources.

IT auditors must recognize the features of consumers of the information system and the decision-making environment in the auditee organization while evaluating the system effectiveness.

IT Audit is the process of collecting and evaluating evidence to find out whether a computer system has been developed to stabilize data integrity, safeguard assets, allows organizational goals to be achieved effectively, and uses resources efficiently. Data integrity relates to the accuracy and completeness of information as well as to its validity in accordance with the norms. An effective information system leads the organization to accomplish its objectives and an efficient information system utilize least resources in attaining the desire objectives. In auditee organization, to evaluate the system effectiveness an auditor must know the user characteristics of information system and decision making environment.

According to (Petter and Suzanne Lovaas, 2012) Information technology verification (audit) Program brochures by the Federal Financial Institutions Examination Council (FFIEC), indicates that a well-structured information verification program essential for the evaluation of management practices, internal control, and finally, respect for the bank's policy regarding I.T. In addition, the audit program should be based on risk, promote critical controls, ensure that the recommendations are addressed in a timely manner, and keep the current Board of Directors on risk management efforts.

Google Translate for Business: Translator ToolkitWebsite TranslatorGlobal Market Finder

***History of IT Auditing*:** Information Technology Auditing (IT auditing) started as Electronic Data Process (EDP) Auditing and developed largely as a result of technology advancement in accounting systems, the need for IT control, and the influence of computers on the ability to perform attestation services. The last few years have been an exciting time in the world of IT auditing as a result of the accounting scandals and increased regulation.

***IT Audit Classification*:** 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, development processes, security protocols and IT governance or oversight. Installing controls are essential but

not adequate to provide sufficient 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.

OTHERS DESCRIBE THE SPECTRUM OF IT AUDITS WITH FIVE CATEGORIES OF AUDITS

Systems and Applications: An audit to verify that systems and applications are proper, are efficient, and are adequately controlled to ensure valid, reliable, timely, and secure input, processing, and output at all levels of a system's activity.

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.

Systems Development: An audit to verify that the systems under development meet the objectives of the organization, and to confirm that the systems are design in agreement with generally accepted norms for systems development.

Management of IT and Enterprise Architecture: An audit to verify that IT management has developed an organizational structure and procedures to ensure information processing in control and efficient environment.

Client/Server, Telecommunications, Intranets, and Extranets: An audit to verify that telecommunications controls are focused three things 1st is on client (computer receiving services), 2nd server, and 3rd on the network connecting the clients and servers.

MATERIALS AND METHODS

Empirical studies are now being undertaken more frequently, as a means of examining a broad range of phenomenon in computer field. A systematic literature review presented in (Dennis J. Gallagher Auditor, 2010) is followed in this research work to conduct the review. This special advisory service report completed the first phase of an Information Technology (IT) audit risk assessment. The purpose of this assessment was to assist in our annual audit planning process to ensure we apply our resources to auditing the highest risk IT areas. The results of the assessment identified specific IT audits which were incorporated into the Auditor's 2011 audit plan.

In developing our approach for the IT audit risk assessment (Dennis J. Gallagher Auditor, 2010) 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. (Dennis J. Gallagher Auditor, 2010) utilized guidance from the Institute of Internal Auditors. (Dennis J. Gallagher Auditor, 2010) 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.

RESULTS AND DISCUSSION

Risk assessing all 338 application systems would have proved to be an unwieldy undertaking and would have laid extra burden on Technology Services personnel. As an alternative to reviewing each application, worked with managers to identify the most critical business systems, as well as, those with the least mature support processes. This led to ranking the risk of a sample of 36 crucial business applications, IT facilities, IT processes, and IT infrastructure. The first phase infers of our IT audit risk assessment process were incorporated into reflected in the plan Attachment A: Listing of Planned Audits.

Audit Title	Department	Audit Type	Audit Objective
DIA Network Security	Denver International Airport	Internal Controls	To evaluate the efficiency and effectiveness of overall network infrastructure security management including but not limited to: firewall, router configuration, patch management, intrusion prevention, detection, logging, event correlation, monitoring, and wireless access configuration management.

OASIS/CAMA IT General Controls	Technology Services	Internal Controls	To assess the effectiveness of the IT General Controls but not limited to: server operating system security (privileged access), server patch management, antivirus controls, change management, user access, vendor support, and system supportability.
OSI IT General Controls and Performance Audit	Technology Services / Denver Police Department	Economy and Efficiency	To assess the efficiency and effectiveness of the IT General Controls supporting the Denver Police System including but not limited to: server operating system security (privileged access), server patch management, antivirus controls, change management, user access, vendor support, and system supportability. The audit scope will include an assessment of National Incident Based Reporting System (NIBRS) for police crime statistics.
Audit Followup	Citywide	N/A	Past audits are surveyed to guaranteed agreed upon audit outcomes and recommendations are being implemented in a timely and effective manner. Although several IT audits may be due for follow-up, they are not specifically called out in the 2011 Audit Plan.

An Evaluation of IT Control/Audit Frameworks

While there are numerous internal controls and IT audit frameworks, it is challenging to find out a framework that can comply with comprehensive criteria for IS measurement. Since the objective of an IS audit is to evaluate IT controls (Mahnic, et al., 2001) a list of existing controls can be evaluated to select context appropriate ones. Here, besides the criteria required, the fame and the extensive usage are looked at while choosing the IT audit framework. "A control framework is a accepted system of control groupings that covers all interior controls expected in an organization" (IIARF 2002, cited in Liu & Ridley, 2005, p. 2) Control frameworks having three categories namely COSO (Committee of Sponsoring Organization) a business oriented controls and SAS (Statement of Auditing Standards); IT focused controls namely ITIL (The IT Infrastructure Library), ISO/IEC 17799:2000 (The International Organisation for Standardisation/the Electro technical Commission) and the Security Code of Conduct; and a third category of controls that align control over IT with business goals namely, COBIT (ibid). In selecting controls businesses have wide choices namely BS 7799, COSO, CoCo, SSE-CMM, FISCAM, GAPP, COBIT, ITCG, GASSP, SAC, and SysTrust and out of these BS 7799, CoCo, ITCG, COSO, FISCAM, COBIT, SAC and SysTrust are goal oriented (Campbell, 2003) with control objectives for each IS entity (process or object of IS for measurement). An internal control provides functional guarantee regarding the attainment of objectives in the area of effectiveness and efficiency of operations, reliability of financial reporting and compliance with regulations (Pathak, 2003). According to Ramos and Pathak (2004, 2003, cited in Brown and Nasuti, 2005) COBIT is the generally adapted standard for IT Governance. Brown and Nasuti (2005), find out three internal control frameworks for IT governance namely COBIT, COSO and eSAC. From Table 2.2, it is evident that COBIT was regarded as a most common framework approved by seven authors along with COSO endorsed by five authors, but the difficulty with COSO is that it gives little help regarding general IT controls (Edelstein, 2004).

CONCLUSION

The model that emerged through the process of researching the associated field from various sources is theoretical and the concept requires to be assessed through empirical research to prove the validity. The nature of the research question directed the researcher to undertake a qualitative study, while the research philosophy pointed towards a positivist paradigm. These directives acted as a basis to go to the next step of selecting a research design and choosing the case study technique. Three studies that were similar to the researcher's topic and the proposed methodology were selected and analysed again to identify the most appropriate way to approach the study. One was not only similar to the research topic, but also conformed to the philosophy, research paradigm and research design. This study was further analysed and selected as a guide. LeCompte's (2000) method of case analysis was adopted. While creating the plan for the analysis, different emerging empirical scenarios

were visualised. But since the upcoming era is always unclear along with the expected answers and the manner of answering (by the respondents), there may be variations in the way the analysis will be done and these will be explained in the relevant report sections. A great deal of work needs to be done before starting the main empirical research. First of all the researcher has to automate the model with both end interface (front end and back end). Secondly while the automated form is being design, IT audit experts need to be contacted for the purpose of identifying the commonly used CO and DCO so that the user can develop a set of questions, and metrics for the expert identified goals. Thirdly the model requires to be tested for usability with a different set of users. Once all of these tasks are completed, the main empirical research can start.

REFERENCES

Brown, W., and F. Nasuti. 2005. What ERP Systems can Tell us about SarbanesOxley. Information Management and Computer Security. 13: 311-327.

Campbell, P. L. 2003. An Introduction to Information Control Models (No.SAND2002-0131). Albuquerque: Networked Systems Survivability & Assurance Department, Sandia National Laboratories.

Dennis J. Gallagher Auditor. 2010. DIA Information Security Management Performance Audit. 201 West Colfax Avenue, Department 705 Denver, Colorado 80202 720-913-5000 FAX 720-913-5247 www.denvergov.org/auditor

Edelstein, S. M. 2004. Sarbanes-Oxley Compliance for Nonaccelerated Filers: Solving the Internal Control Puzzle. The CPA J. 74: 52-58.

LeCompte, M. D. (2000). Analysing Qualitative Data. Theory into Practice. 39: 146-154.

Liu, Q., and Ridley, G. 2005. IT Control in the Australian Public Sector: A 263.International Comparison. Paper presented at the Thirteenth European Conference on Information Systems, Regensburg, Germany.

Mahnic, V., B. Klepec, and N. Zabkar. 2001. IS Audit Checklist for Router Management Performed by Third Party. Paper presented at the International Conference on trends in Communications EUROCON 2001, Bratislava.

Pathak, J. 2003. Internal Audit and E-Commerce Controls. Internal Auditing. 18: 30-34.Petter Lovaas and Suzanne Wagner. 2012. IT Audit Challenges for Small and Medium- Sized Financial Institutions. Annual symposium on information assurance & secure knowledge management, june 5-6, 2012, albany, NY