IJARESM
INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN ENGINEERING, SCIENCE & MANAGEMENT

STUDY ON CHALLENGES AND TECHNIQUES IN CONDUCTING CONCURRENT AUDIT OF INFORMATION SYSTEM

Prof. Ashish Kharvar[1], Prof. Darshan Chauhan[2]

Assistant professor, Computer engineering department, S.N.P.I.T&R.C., Umrakh, Gujarat, India[1]

Assistant professor, Computer engineering department, S.C.E.T.., Surat, Gujarat, India[2]

Abstract*: *Nowadays Information system is an integral part of our life. As the usage of information system grows one need to concern about security and effectiveness of it. Usage of information system has affected traditional auditing and has produced new set of audit challenges for computerized environments. This paper focuses on challenges of conducting concurrent audit of information system and possible techniques to conduct such concurrent audit of information system.

Keywords: Include at least 4 keywords or phrases and should be in Alphabetical Order.

INTRODUCTION

Information system is the most valuable assets of any organization, so its protection from predators from both within and outside is necessary. Hence, there is a need of strong control environment in organization. Certified information system auditor ensures that sufficient control procedures are implemented in an organization.

But information system auditing cant done with traditional procedures because now audit trails is changes as well as information systems are generally concurrent (online) so one can't stop it for auditing purpose which leads to the new issues in audit of information system which is studied in this paper and there few methods to carried out concurrent audit of information system.

NEED FOR AUDIT OF INFORMATION SYSTEM

Factors influencing an organization toward controls and audit of computers and the impact of the information systems audit function on organizations are

- Organizational cost of data loss
- Incorrect decision making
- Cost of computer abuse
- Value of computer hardware, software and personnel
- High cost of computer error
- Maintenance of privacy
- Integrity issue

CHALLENGES OF INFORMATION SYSTEM AUDIT

Audit of information system leads to the following challenges

1. Change in the audit trail and audit evidence:

a. Data retention and storage: client storage capacity may restrict the amount of historical data that can be retained because of that it will be very difficult for an auditor to review and audit the system. Another problem is computer stores data in 0 and 1 so again it is difficult to read and review. Data can be stored in different format like ASCII-7, ASCII-8 etc. so first of all auditor needs to find out this format and then can decode data.

b. Absence of input documents: Transaction data may be entered into directly without the presence of supporting documentation so less paperwork being available for audit examination.

c. Lack of visible audit trail: audit trails in some computer system may exist only for short period of time that makes the auditor's job more difficult.

d. Lack of visible output: output of system is generally in soft copy so auditor needs to access and review these electronic data.

e. Audit evidence: Certain transactions are generated automatically by computer which is not supported by signature of individual so here there is a risk that transaction may be irregular.

f. Legal issues: cyber laws vary from country to country even sometimes between states to state.

2. Change in the type and nature of internal controls:
   Few Internal controls are
   1) Personnel: staff are trustworthy or not, they are doing job to a competent standard or not.
   2) Segregation of duties: it means transaction is split between different people.
   3) Authorization procedure: to ensure that transactions are approved.
   4) Record keeping: the control over the protection and storage of documents, transaction details, and audit trails etc.
   5) Access to assets and records: in the past manual systems could be protected from the unauthorized access through the use of locked doors and cabinets but now a days for computers which are connected to network and internet, increase the risk of unauthorized access.
   6) Management supervision and review: it helps to detect errors and fraud.
3. Changes to Evidence Evaluation: Evaluation of audit trail and evidence is to trace consequences of control's strength and weakness throughout the system.
   1) System generated transactions: Financial systems may have the ability to initiate, approve and record financial transactions.
   2) Automated transaction processing systems: can cause the auditor problems. For example when gaining assurance that a transaction was properly authorized or in accordance with delegated authorities. Automated transaction generation systems are frequently used in just in time' (JIT) inventory and stock control systems : When a stock level falls below a certain number, the system automatically generates a purchase order and sends it to the supplier (perhaps using [Dl technology).

3) Systemic Error: Computers are designed to carry out processing on a consistent basis. Given the same inputs and programming, they invariably produce the same output. This consistency can be viewed in both a positive and a negative manner

CONCURRENT OR CONTINUOUS AUDIT

Different types of continuous audit techniques may be used. Some modules for obtaining data, audit trails and evidences may be built into the programs. Audit software is available, which could be used for selecting and testing data. Many audit tools are also available; some of them are described below:

1) Snapshots Technique: Tracing a transaction is a computerized system can be performed with the help of snapshots or extended records. The snapshot software is built into the system at those points where material processing occurs which takes images of the flow of any transaction as it moves through the application. These images can be utilized to assess the authenticity, accuracy, and completeness of the processing carried out on the transaction. The main areas to dwell upon while involving such a system are to locate the snapshot points based on materiality of transactions when the snapshot will be captured and the reporting system design and implementation to present data in a meaningful way.

2) Integrated Test Facility (ITF): The ITF technique involves the creation of a dummy entity in the application system files and the processing of audit test data against the entity as a means of verifying processing authenticity, accuracy, and completeness. This test data would be included with the normal production data used as input to the application system. In such cases the auditor has to decide what would be the method to be used to enter test data and the methodology for removal of the effects of the IIE transactions.

3) System Control Audit Review File (SCARF): The SCARF technique involves embedding audit software modules within a host application system to provide continuous monitoring of the system's transactions. The information collected is written onto a special audit file-the SCARF master files. Auditors then examine the information contained on this file to see if some aspect of the application system needs follow-up. In many ways, the SCARF technique is like the snapshot technique along with other

4) Continuous and Intermittent Simulation (CIS): This is a variation of the SCARF continuous audit technique. This technique can be used to trap exceptions whenever the application system uses a database management system. During application system processing, CIS executes in the following way:
   - The database management system reads an application system transaction. It is passed to CIS. CIS then determines whether it wants to examine the transaction further. If yes, the next steps are performed or otherwise it waits to receive further data from the database management system.
   - CIS replicates or simulates the application system processing.
   - Every update to the database that arises from processing the selected transaction will be checked by CIS to determine whether discrepancies exist between the results it produces and those the application system produces.

Exceptions identified by CIS are written to a exception log file.

BENEFITS OF CONCURRENT AUDIT

1. Timely, Comprehensive and Detailed Auditing - Evidence would be available more timely and in a comprehensive manner. The entire processing can be evaluated and analyzed rather than examining the inputs and the outputs only.
2. Surprise test capability - As evidences are collected from the system itself by using continuous audit techniques, auditors can gather evidence without the systems staff and application system users being aware that evidence is being collected at that particular moment. This brings in the surprise test advantages.
3. Information to system staff on meeting of objectives - Continuous audit techniques provides information to systems staff regarding the test vehicle to be used in evaluating whether an application system meets the objectives of asset safeguarding, data integrity, effectiveness, and efficiency.
4. Training for new users - Using the ITFs, new users can submit data to the application system, and obtain feedback on any mistakes they make via the system's error reports.

DISADVANTAGES OF CONCURRENT AUDIT

1. Auditors should be able to obtain resources required from The organization to support development, implementation, operation, and maintenance of continuous audit techniques.
2. Continuous audit techniques are more likely to be used if auditors are involved in the development work associated with a new application system. Auditors need the knowledge and Experience of working with computer systems to be able to use continuous audit techniques effectively and efficiently.
3. Continuous auditing techniques are more likely to be used where the audit trail is less visible and the costs of errors and irregularities are high.

REFERENCES

Websites:

[01] http://www.csoonline.com/article/2124025/it-udit/information-systems-audit--the-basics.html

[02] http://rmas.fad.harvard.edu/pages/information-systems-audit

Book:

[03] Ron weber," Information system control and audit

Papers:

[04] International Journal of Information and Education Technology, Vol. 3, No. 3, June 2013, An Information System Audit Model for Project Quality Improvement by the Agile Methodology , Author-Dong Hyup Kim, Dong Soo Kim, Chan Koh, and Hee Wan Kim

[05] Cash, J. I., A. D. Bailey Jr., and A. B. Whinston, "A Survey of Techniques for Auditing EDO-Based Accounting Information Systems," The Accounting Review, October 1977), pp.813-32.