Program Information System Auditing; Theoritical Approach

Ahmadi Aidi

Abstract: Efficient information systems when using fewer resources or minimal in achieving organizational goals are expected. Effective information system capable of completing the organization's objectives. Audit information systems necessary to know the needs of users, whether it is in line with the preparation of the decision-making process

Keyword: Effectively, Efficienty, Decision Making.

1 INTRODUCTION

The information system is used to perform many of the organization's business processes. Interruption or failure of information systems will paralyze the activities of the organization. The role of the information for the organization then the organization becomes very dependent on infromasi and organizations treat information as a resource to avoid the risk that determines whether an organization can continue to operate, (Azhar Susanto, 2013: 11). Issues surrounding the use and management of information systems that still often we find and feel, many instances the implementation of information systems (IS) is problematic. "The end of November 2010, Garuda Indonesia had failed to perform the migration from the old system to IOCS (Integrated Operation Control System) to monitor flight operations, cabin crew and flight traffic. This resulted in chaos Garuda flight schedule for 3 days and thousands of passengers stranded at airports at home and abroad. Garuda allegedly suffered a loss of Rp 250 million and lost profit opportunities of up to Rp 2 trillion, "(Kompas.com, 2012). Another example is the Wikileaks scandal that leaked confidential information, in particular the very important documents of the US government (US). The scandal has made the US and other countries involved angry.. Information collected by Wikileaks comes from internal sources in various US government agencies. Quite apart from whether or not the contents of the document, it shows that in addition to strengthening the technology to fortify the confidentiality of information, monitoring of the human actors of information systems should also be given serious attention, (Info Business, 2014). Problems and obstacles that often occur in the management of information systems include the following: damages for loss of data, losses due to processing computer errors. , making the wrong decision due to incorrect information. , losses due to misuse of computers (computer abused), no maximum utilization value hardware, software and personnel information system.

- *Ahmadi Aidi,*
- *Doctoral students of science accountancy departemen, faculty of economic and business, Padjadjaran University, Bandung, Indonesia and Lecturer of Institut Ilmu Sosial dan Manajemen STIAMI, Jakarta Indonesia, email: ahmadiaidi@yahoo.co.id PH.6285693417298.*

The processed data into information, information is an important asset of the organization. Many organizations rely on information activities. Information for the organization becomes a portrait of conditions in the past, the present and the future. If information is missing it will result in a loss for the organization, because there is no adequate control, (Jack J Champlain, 27, 2003). Processing data using a computer be the primary focus in computer-based information systems. Many organizations have been using the computer as a means to improve the quality of their work, ranging from a simple task, such as data input through the use of computers as an aid for the leadership to take a decision. Unit jobs in the organization already interconnected and integrated, but can occur any damages, if the process in the computer errors occur, (Jack J Champlain, 2003). Losses range from data that can not be trusted until the error process of implementation. The quality of a decision depends on the quality of information presented to the decision. The level of accuracy and the importance of a data or information from work unit below it depends on the type of decision to be taken by each head unit are working on it. Often times the crime computer misuse. Some types of crime and computer misuse include viruses, hacking, direct access that is not legal for example go to the computer room without permission or using a computer terminal so as to cause physical damage or retrieve data or computer programs without permission. Unauthorized access to the personal interests of an individual who has the authority to use the computer, but for the purposes of improperly. In an existing information systems to organizations such as hardware, software, data and user is the organization's resources. There are several units in an organization who are big spending to invest in the preparation of an information system, but there are still weaknesses in the continuing process implementation because of the use of information technology (IT) in each unit depends on the policiies of its leader. Information system problems such as the above should have been anticipated. If it can not be prevented, then the organization should have a plan to minimize the impact and recover, this is where the important role of information systems auditing. Audit ensures the reliability and availability of information systems in helping achieve organizational goals effectively by utilizing the resources of the organization efisen. The audit program is designed to address the major risk in virtually all computing systems, therefore it is important that this topic be used as the title of this article.

2 LITERATURE RIVIEW

2.1 Audit

Auditing is the process by which competent, independent person accummulate and evaluates evidance about quantifiable information related to a spesific economic entity for the porpuse of determining and reporting on the degree of corespondence between the quantifiable information and established creteria, (A.Aren Alvin and James K.Loebbecke:1991:2). Auditing is systematic process of objectively obtaining and evaluating evidence regarding assertions about economic actions and events to assertions the degree of corespondence between those assertions and established creteria and communicating the results to interesting user, (Messer.F William:1997:8). Auditing is a series of practise and procedures method and technique, away of doing with little need for the explanations descriptions, reconciliations and arguments so frequantly lumped together as theory, (Mautz.RE ;1993:1) Based on the above definition can be synthesized that an audit is gathering evidence about information to determine and report the degree of correspondence between the information with the criteria established.

2.2 Program Audit

An audit program is a detailed list of the audit procedures to be performed in the course of the examination, (Whittington, Pany and Meigs,1992:340). The audit program for most audist is design in three parts:

a) Test of transaction.
b) Analytical procedures.
c) Test of detail of balances.

A set of instructions for carrying out the audit plan, is contains a detailed description of the decesion the auditor has made regarding:

a) The audit procedures to be used.
b) The size of each sample.
c) The method chosen for selecting the item to examine.
d) The proper timing of each audit procedures.

The audit program conducted with the aim that the audit process can be carried out effectively and efficiently, (Jack J Champlain, 2003:29). Based on the above definition can be synthesized that an audit program is necessary to conduct an effective and efficient audit. Audit program is essentially a checklist of various tests that the auditor should conduct the audit scope Based on the results of tests performed, the auditor should be able to determine the adequacy of control during certain processes.

2.3 Audit Procedure

Audit procedure consists of six stages as shown in Figure 1 below,

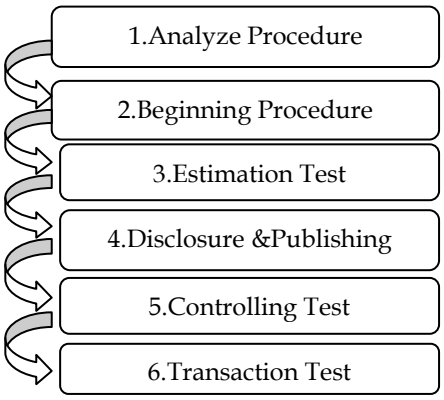

Figure 1. *Audit Procedure Steps*
Source: *William F Messer,1997:8*

2.4 System

The system is a collection of people who cooperate with the provisions of the rules of systematic and structured to form a single entity perform a function for the purpose, (Mc.Leod, 2004). The same thing was stated by (Azhar Susanto, 2013: 22), that the system is a collection / group of sub-systems / parts / components in any physical or non-physical are interconnected with each other and work together in harmony to achieve a certain goal. Based on the above definition it can be concluded that the system is a collection of people or a collection of sub sisitem good physical shape maupaun non-physical working together in harmony to achieve a goal of the organization or company.

2.5 Information

Information is data that is processed into a more useful and meaningful for the recipient and to reduce uncertainty in the decision making process regarding a situation, whereas, according to Azhar Susanto (2013: 38), information is the result of data processing that gives meaning and benefits. So it can be concluded that the information is processed data that can benefit the decision-making process.

2.6. Information System

The information system is a collection of subsystems of both physical and non physical are interconnected with each other and work together in harmony to achieve one goal of process data into useful information, (Azhar Susanto, 2013: 52). The information system is a collection of components that are interconnected and cooperation to collect, process, saving and disseminate information to support decision-making, coordination, control, and to provide an overview of activity within the company, (Laudon, 1998). The system is a combination of computer and user that managing change data into information, and saving the data and the information, (Mc Keown, 1993). The information system is a system that has the ability to gather information from all sources and uses various media to display information, (Mc Leod, 2004). Based on the above definition can be synthesized that the information system is a tool that consists of software, hardware, human resources, computer to help organizations to analyze data for the preparation of the decision-making process.

2.7. Information System Audit

Ron Weber (1999:10), " Infirmation system auditing is the process of collecting and evaluating evidence to determine whether a computer systems safeguards assets, maintains data integrity, achieves or- ganzational goals effectively, and consumes resources effiently". Information systems auditing is the process of collecting and evaluating evidence to determine whether a system of computerized applications have established and implemented a system adequate internal controls, all assets are well protected or not misused and ensuring data integrity, reliability and effectiveness and efficiency of computer based information system.

3. DISCUSSION

3.1. Goal of Information System Auditing

According to Ron Weber (1999:11-13) can be summed up in outline information systems auditing purposes is divided into four, namely:

a) Enhance the security of information systems assets
b) Improve data integrity
c) Improving the effectiveness of the system.
d) Improving the efficiency of the system.

Enhance the security of information systems assets

Assets information systems within an organization include hardware, software, facilities and human resources including knowledge, data files, system documentation and equipment. Are all assets such as the above have been protected by a system of internal control. Hardware can be destroyed, proprietary software and contents stolen, equipment can be used by unauthorized parties. All assets was concentrated in one location or in a location that is small as in a single storage so that it can be kept safely.

Improve data integrity

Data integration is a fundamental concept in information systems auditing, if the data can be maintained its integrity, the organization will excel and avoid defeat in the competition. There are three factors that affect the value of the data within an organization, as shown below:

a) The data of individual decision-makers.

A data load on the ability of decision makers to make changes with the decisions that are influenced by the environment of uncertainty.

b) Data sharing between decision makers.

c) Values of data to competitors.

If a data value is given to the competitors then it is a disadvantage and would interfere with the organization's position in the existing market share

Improving the effectiveness of the system.

An effective information system capable of completing the organization's goals. Evaluate the effectiveness of information systems necessary to know the needs of the user. The effectiveness of the enterprise information system has an important role in the decision making process. An information system can be said to be effective when the information system in accordance with user needs.

Improving the efficiency of the system.

Efficienty information systems are using resources when little or minimal in achieving the goals of the organization is expected. The decline in system performance of individual applications will lead to increased user frustration then management must decide whether efficiency can be enhanced or additional resources need to be purchased. Efficiency becomes very important when a computer no longer has sufficient capacity

3.2. The necessity of Control and Information System Audit

According to Weber, (1999: 6) The factors that drive the importance of control and audit of information systems, among other things:

a) Detecting that the computer is not managed in a less directional.
b) Detecting the risk of data loss.
c) Detecting the risk of making the wrong decision due to a computerized information processing system is wrong slow and incomplete.
d) Maintain asset value of the company for hardware, software and personnel are typically high.
e) Detecting the risk of a computer error.
f) Detecting the risk of computer misuse (fraud).
g) Maintain confidentiality.
h) Increase control of the evolution of the use of computers.

3.3. Steps program information systems auditing.

According to Champlain, Jack, J, 2003.32, steps in the program information systems auditing, into four categories, namely:

A. Test of Environmental controls.
B. Test of Physical security controls.
C. Test of Logical security controls.
D. Test of Information System operating controls.

A. Test of Environmental controls.

Step 1. Assess the adequacy and effectiveness of the organization's IS security policy. In addition, assess whether the control requirements specified in the organization's IS security standards adequately protect the information assets of the organization. At a minimum, the standards should specify the following controls and require them to be applicable to all information systems:

a. The maiden password should be changed after the system is installed.
b. There is a minimum password length of eight or more characters.
c. Passwords require a combination of alpha and numeric characters.
d. The password is masked on the screen as it is entered.
e. The password file is encrypted so nobody can read it.
f. There is a password expiration period of 60 days or less.
g. Three or fewer unsuccessful sign-on attempts are allowed, then the user ID is suspended.
h. User sessions are terminated after a specified period of inactivity (e.g., five minutes or less).
i. Concurrent sign-on sessions are not allowed.
j. Procedures are in place to remove user IDs of terminated users in a timely manner.
k. Users are trained not to share or divulge their passwords with other users, post them in their workstations, store

them in electronic files, or perform any other act that could divulge their passwords.

l. Unsuccessful sign-on attempts and other logical security-related events (e.g., adding and deleting users, resetting passwords, restarting the system) are logged by the system, and the log is reviewed regularly by system security staff.

m. Fully developed and tested backup and recovery procedures exist to help ensure uninterrupted business resumption in the event of a full or partial disaster.

n. New information systems are required to be designed to enable the aforementioned controls to be implemented by system security administrators. New systems include those developed in house, those purchased from vendors, and third-party processor systems. In the case of software vendors and third-party processors, the above control requirements should be specified as requirements in the contract.

Step 2. For service organization applications, examine the most recent report on the policies and procedures placed in operation at the vendor's data processing site as prepared by its external auditors. In the United States, the format and testing requirements are dictated by Statement on Auditing Standards 70 (SAS 70), issued by the American Institute of Certified Public Accountants. SAS 70 reports may also describe tests of the operating effectiveness of the policies and procedures if the vendor has contracted the external auditor to do so.

a. Assess the adequacy of controls described in the report and determine whether applicable control recommendations have been implemented at your organization.

b. If applicable, determine whether another type of security or privacy certification exists (e.g., TruSecure, SysTrust, WebTrust, BBBOnline, TRUSTe).

Step 3. If the system was purchased from and supported by a vendor, assess the financial stability of the system vendor using the most recent audited financial statements prepared by the vendor's external auditors. (Optimally, this step should be performed prior to when the decision is made to purchase the system. Otherwise, significant resources could be wasted on a system for which the vendor will no longer exist.)

a. Select a sample of recent invoices from the system vendor and determine whether costs have been properly recorded and classified on the financial statements of your organization. Costs should normally be amortized over the expected useful life of the system.

b. For IS development projects, determine whether applicable internal development costs (e.g., programmer hours) have been capitalized and amortized over the estimated useful life of the internal use system in accordance with AICPA Statement of Position (SOP) 98-1 (does not apply to software sold to external parties). See Chapter 15 for details on IS development projects.

Step 4. Examine the vendor software license agreement and any agreements for ongoing maintenance and support to ensure that they are current, address service needs, and do not contain or omit any wording that could be detrimental to your organization. Where applicable, the agreements should also require that a copy of the programming source code of the current version of the software be stored in escrow by an independent third party so that it is available to your company in the event the vendor goes out of business or another stipulated event occurs (e.g., breach of contract; software no longer supported by vendor).

B. Test of Physical security controls.

Step 5. Assess the adequacy of physical security over the computer system hardware and storage media.

Step 6. Determine whether an adequately trained backup system security administrator has been designated.

Step 7. Assess the adequacy and effectiveness of the written business resumption plan, including the results of mock disaster tests that have been performed.

a. Assess the adequacy of backup procedures for system software and data. The procedures should include periodic backups as necessary (daily, weekly, monthly), off-site storage at a secure location, and rotation of backup media.

b. Verify that at least one alternative set of processes exists for each key assumption (transportation, communications, staffing, processing facilities, etc.).

Step 8. Assess the adequacy of insurance coverage over the hardware, operating system, application software, and data. Hardware should be covered at replacement cost. The costs of re-creating any lost software and data should be covered. Optimally, coverage should include lost revenues directly resulting from hardware failure and loss of the operating system, application software, and data during covered events.

C. Test of Logical security controls.

Step 9. Determine whether the maiden password for the system has been changed and whether controls exist to change it on a periodic basis in conformity with the computing system security policy, standards, or guidelines identified in Step 1.

Step 10. Observe the system security administrator sign on and print a list of current system users and their access capabilities. Alternatively, if you can obtain appropriate system access, you can obtain the list of users independently.

a. Assess the reasonableness of the access capabilities assigned to each user.

b. Confirm that user IDs of terminated employees are suspended in a timely manner.

c. Confirm that system access capabilities of transferred employees are adjusted accordingly.

Step 11. Document and assess the reasonableness of the default system security parameter settings. The settings should conform to the organization's computing system security policy, standards, or guidelines tested in Step 1. (Be alert to the fact that in some systems, individual user parameter settings override the default system security parameter settings.)

Step 12. Test the functionality of the logical security controls of the system (e.g., password masking, minimum password length, password expiration, user ID suspended after successive invalid sign-on attempts, log-on times allowed, and

session time-outs).

Step 13. Determine whether the file containing user passwords is encrypted and cannot be viewed by anyone, including the system security administrator.

Step 14. Determine whether sensitive data, including passwords, are adequately encrypted throughout their life cycles, including during storage, transmission through any internal or external network or telecommunications devices, and duplication on any backup media.

Step 15. Assess the adequacy of procedures to review the log of system security-related events (e.g., successive invalid sign-on attempts, system restarts, changes to user access capabilities and user parameter settings).

Step 16. Assess the adequacy of remote access controls (e.g., virtual private networks [VPNs], token devices [CRYPTOCard, SecurID, etc.], automatic dial-back, secure sockets layer [SSL]).

D. Test of Information System operating controls.
Step 17. Determine whether duties are adequately segregated in the operating areas supporting the information system (e.g., transactions should be authorized only by the originating department, programmers should not have the capability to execute production programs, procedures should be adequately documented, etc.).

Step 18. Determine whether there have been any significant software problems with the system. Assess the adequacy, timeliness, and documentation of resolution efforts.

Step 19. Assess the adequacy of controls that help ensure that IS operations are functioning in an efficient and effective manner to support the strategic objectives and business operations of the organization (e.g., system operators should be monitoring CPU processing and storage capacity utilization throughout each day to ensure that adequate reserve capacities exist at all times).

4. Conclusion

Based on the description above it can be concluded that:

1. The existing information assets must be protected properly from the risk of damage, loss, errors or misuse.
2. The information to be processed can be assured integrity means must be complete and must be accurate.
3. The information system developed must be a solution that is able to achieve its objectives and help achieve organizational goals effectively.
4. Resources information systems and technology owned devices must be used efficiently and to be responsible.

Acknowledgments

I would like to thank the reviewers who have agreed and accepted this paper. I also would like to say many thank to my lecturer Prof. Dr. Azhar Susanto,SE.Ak,M.Buss,CPA,CA and Rector Institute STIAMI Dr.Ir.Panji Hendrarso.MM, for the guidance and also thank to my colleagues at Doctoral Program Science of Accountancy Padjadjaran University - Bandung - Indonesia.

References

[1] Arens, A.A., J.K. Loebbecke. Auditing: An Integrated Approach. Eight Edition. New Jersey: Prentice Hall International Inc,pp.2,1991.

[2] Azhar Susanto, Sistem Informasi Akuntansi,, Lingga Jaya Bandung,pp.11,22,38,52,2013.

[3] Champlan,Jack,J,Auditing Systems ,Second edition ,Jhon Willey and Son Inc, New Jersey Canada,pp,27-29-30-32,2003

[4] Loudon, Management Information System: New approach to organizations and technology, 5th, Prentice Hall International,Inc USA,1998

[5] Mc.Leod, Management Information System, 9th, Prentice Hall, USA,2004.

[6] Mc Keown, Management Information System: Managing With Computer, The Dryden Press,USA, 1993.

[7] Messier, F.W., Auditing a systematic approach, Library of congress cataloging in publication data.pp,8,1997

[8] Meigs,Whittington,Pany and Meigs, Principles of Auditing, Library Congress of cataloging in Publication Data,pp,340-344,1992.

[9] RE Mautz, The Philosophy of Auditing, American Accounting Assosiation,pp,1,1993.

[10] O.Brien, Management Information System: Managing Information Technology in the internetworked Enterprise, 6th, Mc Grow Hill,USA,2004.

[11] Weber, Information System Control and Audit, Prentice Hall International Inc,USA,pp,6-10-11-12-13,1999.