The improvement of IT auditor's human resources for audit quality

Bonifasius H. Tambunan[1,*], Halomoan Sihombing[1], Lastri[2]

[1]Doctoral Student, Accounting Department, Universitas Sumatera Utara, Jln. Dr. Mansur, Medan.
[2]Development Economic Department, Universitas HKBP Nommensen, Jln. Sutomo, Medan

*tambunanbonifasius@gmail.com

Abstract. The growth of Information Technology has adopted on the various sector, including auditing world. With IT adoption, there are needed for IT auditors that understand the audit through the computer or audit the client's financial application. This research aims to discuss how to improve the IT auditor's human resources to increase the audit quality. The method that used at the research is the descriptive method with literature study to explain the competence of an IT auditor. The result shows that there are three guides that IT auditor must follow to intensify their skills. Firstly is CISA certification and training material. Secondly is CISA continuing certification and education requirement. The last is COBIT Framework, Control Objectives M2, M3, and M4. Specifically for Indonesia, there is one additional guide, which is Indonesian National Competency Standards.

1. Introduction

In recent years, the Information Technology and System have grown rapidly. Most of the business has adopted the information technology into their systems, including accounting system. The use of the Accounting Information System has assisted the accounting procedure itself. The more progress for information technology and system, the more it influences to the accounting systems. It shows on the changing of processing the data, from manual systems to computerized systems (Marwanto, 2010). Several of accounting software such as MYOB, Zahir Accounting, Accurate Accounting, and Bee Accounting has use widely. In general, the accounting processes in both manual and computerized are same. The difference is that the process usually done separately in the manual process will be incorporated computerized in the SIA so that the processing time becomes shorter.

With the data input process that changed from manual to the computerized system, then the company's Internal Control System also turned into computer-based Internal Control. It also affects the audit process whereby the auditor must use the financial statements generated from the computerized process as well as the accounting stages employed by the computer as a basis for determining audit opinions.

The adoption of information technology does not only occur in the field of accounting alone. The field of auditing also began to slowly adopt information technology. The auditor does not usually check all the evidence and transaction documents and thus must rely on the reliability of the Company's Internal Control System. If the company already uses information technology as a recording system, then the auditor must also understand the accounting process through information technology so they can generate an appropriate audit

opinion. In addition, previous auditors work outside the computer with a focus on the output of the internal control, assuming if the results of the output are reliable, then the process of producing output can also be said reliable (Yani, 2009). With the existence of information technology, emerged a new approach in the audit Computer Assisted Audit Tools (CAATs).

The audit process that executed manually now has been done through the computer. CAATs soon became a prima donna in terms of an audit because it has the following advantages (Senft and Gallegos, 2009):

a. Increase auditor productivity because auditors are able to do routine work more quickly and focus on important issues in financial statements
b. Jobs that cannot be completed manually can be done by the computer
c. Reduce costs due to reduced audit completion time
d. Improve the client's competitive edge
e. Able to do difficult things without having to add staff

With these conditions, then the need for auditors who understand the IT audit becomes an important and urgent thing. The better an auditor's understanding of IT, the better the audit process will be done so that the results of the audit given quality and can be trusted. This is because an auditor is expected to evaluate the level of effectiveness and efficiency of a system. By having these capabilities the auditor can obtain a favorable position along with the development of information systems such as today (Wilkinso, 2000).

The ability of IT auditors can be seen from their ability to meet the competency requirements in IT audit field. The question is what is the core competencies for IT auditor? How the IT auditors achieve the competence standard to do a better audit in an application? This study aims to discuss the competency standards that must be owned by an IT auditor to be able to carry out the IT audit process well in the international world in general and in particular in Indonesia.

2. Literature Review

Information Technology Audit

Information technology audit is the process of collecting data and evaluating the evidence to determine whether a computerized application system has established and implements an adequate internal control system, all assets are well protected or misused and ensured data integrity, reliability and effectiveness and efficiency of the operation of information-based systems computer (Kajian Pustaka, 2014).

Audit Quality

Meutia (2004) defines audits as a process to reduce the misalignment of information available between managers and shareholders by using outside parties to authorize financial statements. DeAngelo (1981) defines audit quality as a combined probability for detecting and reporting material errors in financial statements. Audit quality is seen as an ability to enhance the quality of financial reporting of a company. With high audit quality is expected to increase investor confidence.

IT Auditor Personal

Personnel including all human resources in work units related to the organization of electronic systems being audited. According to Dessler (2010: 5), Human Resource Management is the process of obtaining, training, assessing, and compensating employees, taking into account their working relationships, health, security, and justice issues.

IT Auditor Qualification

Competence is a professional skill possessed by the auditor as a result of formal education, professional examination as well as participation in training, seminars, symposia and others

3. Research Method

This research uses the qualitative approach with research method used is the analytical descriptive method. The data collection techniques used in this research are:

a. Literature study, which is done by reading literature book about the audit of Computer-Based Accounting Information System, SKKNI auditor of IT field, and doing searching data about HR qualification in IT auditor field.
b. Observation, which is done by taking the secondary data contained on the internet then analyze the data.
c. Conclusion. After the analysis process has been completed, then the conclusion is drawn by drawing conclusions from the data analysis that has been done before

4. Result and Discussion

In the standard S4 IT audit issued by the Information Systems Audit and Control Association (ISACA, 2010), there are two standards relating to an IT auditor's professional competence. Those standards are:

a. An IT auditor must have professional competence and expertise, as well as capabilities and knowledge that support the conduct of the audit. Through this standard, the IT auditor is required to prove that he is proficient and has the ability to audit client applications. If not, then the auditor should refuse to audit.
b. An IT auditor must continue to develop his professional competencies through continuing education and training. Under this standard, the auditor must meet the minimum requirements for continuing education and training. Every IT auditor should be through formal education, training, and experience.

Additionally, ISACA standards mention the competency guidelines an IT auditor must possess. The guides are:

a. CISA certification and material
b. CISA continuing certification and education requirement
c. COBIT Framework, Control Objectives M2, M3, and M4.

In particular, Indonesia has set competency standards for IT auditors to comply with the Indonesian National Work Competence Standards (SKKNI), as outlined in Ministerial Decree of Employment No. 48/2015. This regulation governs 15 competencies to be met by every IT auditor in Indonesia.

CISA Certification and Material

The first guide referred to by ISACA in terms of IT auditor competence is CISA (Certified Information System Auditor) certification. The CISA certification was issued by ISACA since 1978 after the participants have passed the exam held by ISACA (Pusilkom UI, 2018).

CISA is an internationally recognized certification in the field of IT audits and in the field of Supervision and Security to enhance the expertise in the field of information system auditing. An IT auditor with CISA certification has been recognized as having a standard and a guarantee for the prerequisite of competency assessment in the field of information system and information technology audit (Pusilkom UI, 2018).

CISA certification is made for auditors auditing the level of effectiveness and efficiency of the use of information technology by companies. CISA certified auditors have an obligation to ensure that the system has been designed, developed and implemented to support the business needs and objectives of the company. A CISA auditor must understand the concept of IT auditing, not just a definition.

CISA certification will be awarded by ICASA if it has passed the exam held by ISACA. The material tested in CISA certification consisting of five domains (Pusilkom UI, 2018), namely:

a. The Process of Auditing Systems. In this domain, an IT auditor must prove that he is capable of providing audits in accordance with the information system audit standards to help clients protect and monitor the use of information systems.
b. Governance and Management of IT. This domain requires the auditor to understand and can provide assurance that the information system run by the client is in accordance with the goals and assist client strategy.
c. Information System Acquisition, Development and Implementation. This domain aims to determine the ability of auditors to prove the suitability between the use, development, and implementation of the information system used by the client is in accordance with the goals and strategies of the company.
d. Information Systems Operations, Maintenance and Service Management. Domain exam is intended to determine the ability of auditors in terms of the process of checking the suitability between the operating system, maintenance, and service of applications run auditors are in accordance with corporate goals and strategies.
e. Protection of Information Assets. This domain aims to prove the auditor's ability in terms of security policy checks, standards, procedures, and monitoring of information systems.

To obtain CISA certification, the requirements to be completed are:

a. Pass the CISA exam
b. Submit an application for CISA certification
c. Minimum 5 years’ experience in auditing, controlling, or securing information system
d. Comply with ISACA professional codes of conduct
e. Comply with CISA Continuing Education and Training
f. Meet the information system audit standards

CISA continuing certification and education requirement

One of professional auditors code of ethics is the auditor must have the competence and professional expertise to bias provide audit services to clients. An auditor should follow a series of year-round training to continually improve auditor skills and expertise. This requirement also applies to any CISA certification holder.

The second reference in terms of the Information Systems Audit Standards is CISA Education and Training. After obtaining CISA certification, the certification holder must meet CISA's continuing education and training requirements in order to maintain the certification annually.

It aims to maintain the quality of new levels and knowledge of each CISA certification holder in the areas of auditing, monitoring and securing information systems. The CISA certification holder must meet the following qualifications in connection with Education and Sustainable Training (ISACA, 2018):

a. Following at least 20 hours of training and continuing education of each year.

b. Follow the PPL at least 120 hours within three years
c. Does not violate the ISACA Professional Code of Conduct
d. Does not violate ISACA Information Technology Auditing Standards.

The activity that accepted by the CISASA Certification Committee and may be recognized as training and continuing educations are as follows (ISACA, 2018):

a. Training and continuing education, including activities organized by ISACA. This category includes conferences organized by ISACA, seminars, workshops, and similar activities held by ISACA. For this point, there is no maximum activity hour's limit. The point is that every hour of ISACA activity followed can be reported as training and continuing education.
b. Training and continuing education held by other than ISACA. Examples of such activities are training, conferences, seminars, workshops, and other activities not sponsored by ISACA. This activity will also not have the maximum limit that can be reported. However, for this category, activities recognized as training and continuing education are just activities that increase the knowledge of CISA certification holders in terms of audit, supervisory, and development of information systems and other matters relating to information systems.
c. Self-help course. This activity also does not have a maximum reporting limit and will only be recognized as training and continuing education if the course adds to the knowledge of the CISA certification holder in terms of auditing, supervising and developing information systems and other matters relating to information systems.
d. Product sales or marketing presentations. This activity is included in the process of selling products or systems related to the assessment of information systems. The maximum hour of activity that may be admitted as training and continuing education is 10 hours.
e. The teaching process related to the information system. This activity has no reporting limit and the recognition of the clock will be doubled. The point is if there is involvement in teaching for five hours, then the recognition of training and continuing education hours is as much as 10 hours.
f. Publication. This activity will be recognized if the published publications relate to the information system. Publications may be in the form of journals, books, or scientific papers. This activity has no maximum reporting limit.
g. CISA exam review. There is no maximum reporting limit in this activity.
h. Pass another professional certification. If the CISA certification holder takes another certification exam related to the information system, this activity may be recognized as training and continuing education. Each test hour will be recognized as two hours of PPL
i. Working as a Board or Committee at ISACA. This activity includes active participation in ISACA councils, committees, committee representatives, task executives, or participation in representatives of ISACA. The maximum acceptable hourly limit is 20 hours for each certification issued by ISACA.
j. Contribution in terms of audit profession and supervision of information systems. The maximum reporting hour limit is for 20 hours for all activities.
k. Mentoring. This activity is included in coaching, reviewing, or assisting the CISA exam. The maximum recognized reporting hour limit is for 10 hours.

COBIT 5

According to Azizah (2017: 377), an information system audit is a process of collecting and evaluating evidence to determine whether the information system determines and implements an adequate internal control system, all assets are well protected and not abused and ensured data integrity, reliability and effectiveness and efficiency of implementation Computer based information system. Tools that can be used to audit information systems are using the COBIT framework. COBIT is a framework for building IT Governance. With reference to the COBIT framework, an organization is expected to be able to implement IT governance in achieving its goals. IT governance integrates the optimal way of planning and organizing, implementing, supporting and monitoring process of Information Technology performance.

COBIT serves as a standard guide to help the manager to manage an organization to achieve its goals by utilizing IT. COBIT provides guidance on a framework that can control all organizational activities in detail and clear so that it can help facilitate decision making at the top level within the organization. COBIT has 4 Domain Coverage:

1. Planning and Organization (Plan and Organization). This domain includes strategies and tactics concerning the identification of how IT can best contribute to the achievement of the organization's business goals so as to establish a good organization with good technological infrastructure
2. Procurement and Implementation (Acquire and Implement). To realize IT strategy, IT solutions need to be identified, built or acquired and then implemented and integrated in business processes.
3. Deliver and Support. This domain relates to the desired service delivery, which consists of operations on security and business continuity aspects up to training procurement.
4. Monitoring and Evaluation (Monitor and Evaluate). All IT processes need to be assessed regularly and periodically how their quality and compliance with control needs.

In Monitoring and Evaluation, all IT processes need to be assessed regularly and periodically how to be qualified and appropriate to monitoring needs. The framework of the 4th domain of COBIT is:

M1: Monitor the Processes

It needs to satisfy the business requirement to ensure the achievement of the performance objectives set for the IT processes, it definition of relevant performance indicators, the systematic and timely reporting of performance and prompt acting upon deviations and takes into consideration:

a. Scorecards with performance drivers and outcome measures
b. Customer satisfaction assessments
c. Management reporting
d. Knowledge base of historical performance
e. External benchmarking

M2: Assess Internal Control Adequacy

Assessing internal control adequacy that satisfies the business requirement to ensure the achievement of the internal control objectives set for the IT processes is enabled by the commitment to monitoring internal controls, assessing their effectiveness, and reporting on them on a regular basis and takes into consideration:

a. Responsibilities for internal control

b. Ongoing internal control monitoring
c. Benchmarks
d. Error and exception reporting
e. Self-assessments
f. Management reporting
g. Compliance with legal and regulatory requirements

M3: Obtain Independent Assurance

This object is use to obtaining independent assurance that satisfies the business requirement to increase confidence and trust among the organization, customers, and third-party providers is enabled by independent assurance reviews carried out at regular intervals and takes into consideration as following:

a. Independent certifications and accreditation
b. Independent effectiveness evaluations
c. Independent assurance of compliance with laws and regulatory
d. Requirements
e. Independent assurance of compliance with contractual commitments
f. Third-party service provider reviews and benchmarking
g. Performance of assurance reviews by qualified personnel
h. Proactive audit involvement

M4: Provide for Independent Audit

It providing for independent audit that satisfies the business requirement to increase confidence levels and benefit from best practice advice is enabled by independent audits carried out at regular intervals and takes into consideration:

a. Audit independence
b. Proactive audit involvement
c. Performance of audits by qualified personnel
d. Clearance of findings and recommendations
e. Follow-up activities
f. Impact assessments of audit recommendations (costs, benefits and Risks)

Indonesian National Working Competency Standards on Field of Information Technology

In addition to the 3th professional competence guides IT auditor issued by CISA, in Indonesia set an additional standard that is Standar Kompetensi Kerja Nasional Indonesia (SKKNI) or the Indonesian National Work Competency Standards. SKKNI is based on the Decree of the Minister of Employment of the Republic of Indonesia Number 48/2015. The Competency Standards that must be owned by the IT Auditor are:

1. Analyze Information Technology Audit Risk
   Elements of competence: Identify environment, boundaries, and information technology assets audited; analyze the risks associated with information technology being audited
2. Preparing the Information Technology Audit Procedure Plan
   Elements of competence: Identify the information technology-related controls to be tested; establish an information technology audit testing procedure
3. Allocate Information Technology Audit Resources

Elements of competence: Estimate the needs of information technology audit resources; Allocate information technology audit resources; Allocate information technology audit resources

4. Implementing the Audit Procedures for Information Technology Planning
   Elements of competence: Describe the control of information technology planning; Evaluating the design of information technology planning; testing the implementation of information technology planning controls; Analyze the test results Control of information technology planning
5. Implement the Audit Procedure for Information Technology Development
   Elements of competence: Describe the control of information technology development; Evaluate the design of Information Technology development control; Testing the implementation of information technology development control; Analyze the test results of information technology development control
6. Implement the Audit Procedure of Information Technology Operations
   Elements of competence: Describe operational control of information technology; Evaluate the design of operational control of information technology; test the implementation of information technology operational controls; Analyze the results of operational control testing of information technology
7. Implementing the Audit Procedure for Monitoring of Information Technology
   Elements of competence: Describe Control of monitoring of information technology; Evaluate the design of Information Technology monitoring control; Testing the implementation of information technology monitoring control; Analyze the test results Control of monitoring of information technology
8. Implementing an Audit Procedure on Information Technology Applications
   Elements of competence: Describe the control of information technology applications; implementing an Audit Procedure on Information Technology Infrastructure
   Elements of competence; Evaluating the design of information technology application control; Testing the implementation of information technology application control; Analyze the test results of information technology application control
9. Implementing the Audit Procedure on Information Technology Infrastructure
   Elements of competence: Describes information technology infrastructure control; evaluate the design Control of technology infrastructure
   Information; Testing the implementation Control of technology infrastructure Information; Analyze the results of IT infrastructure information technology control Tests; Evaluate the feasibility of implementing information technology audit procedures
10. Supervise the Feasibility of Implementation of Information Technology Audit Procedure
    Elements of competence: Describe the procedure planned information technology audit;
11. Monitoring the Feasibility of Documentation of Implementation of Information Technology Audit Procedure
    Elements of competence: Identify documentation of results of information technology audit procedures; Evaluate the feasibility of documentation of the results of information technology audit procedures
12. Preparing Information Technology Audit Results
    Elements of competence: Compile the results of the implementation of information technology audit procedures; Prepare reports on the results of information technology audit procedures
13. Developing an Information Technology Audit Recommendation

Elements of competence: Analyze the weaknesses of information technology control; Prepare information technology audit recommendations

14. Identify Information Technology Audit Follow Up
    Elements of competence: Analyze information technology audit recommendations; Describes follow-up audit of information technology
15. Verify the Feasibility of Follow-Up of Information Technology Audit
    Elements of competence: Identify evidence of follow-up audit of information technology; Analyze the feasibility of advanced information technology audits

5. Conclusion

From the discussion, it can be concluded that:

a. The quality of an IT auditor will greatly affect the quality of audits carried out
b. There are three internationally competent units to be followed by an IT auditor, namely CISA certification, CISA Certification PPL, and COBIT Framework Control and Objective.
c. Especially for Indonesia, every IT auditor in Indonesia is required to have competence as defined in SKKNI field of auditor of Information Technology through Ministerial Decree of Employment No. 48/2015.

Based on these conclusions, the author's suggestions are as follows:

a. For every IT auditor, it is expected to maintain and improve its competence in order to produce a good audit quality.
b. It is expected that the IT auditor will participate in the certification and PPL CISA in order to increase the competency level.
c. For IT auditors in Indonesia, to maintain competence as defined in SKKNI.

References

[1] Kajian Pustaka, 2014, *Audit Sistem Informasi* [Information System Audit](Online). https://www.kajianpustaka.com/2014/02/audit-sistem-informasi.html Accessed on April 25th, 2018 at 19.58 Indonesian time.

[2] Marwanto, 2010, *Peranan Teknologi Informasi Dalam Perkembangan Audit Komputerisasi.* [The Role of Information Technology on the Development of Computerized Audit]. *Jurnal EKSIS Vol. 2 (2), Agustus 2010, pp:1440-1605.*

[3] Yani, A., 2009, *Audit Sistem Informasi Akuntansi Berbasiskan Komputer* [Information Sytem Audit on Computer Bassed]. *PERSPEKTIF Vol. 7 (2), September 2009, pp: 1-11.*

[4] Senft, S., dan Gallegos, F., 2009, *Information Technology Control and Audit*. Boca Raton: Auerbach Publications.

[5] Wilkinson, J.W., Cerullo, M. J., Raval, V. & Wong-On-Wing,B. 2000. Accounting Information Systems- Essential Concepts and Applications, Fourth Edition, John Willey and Sons, Inc.

[6] ISACA, 2010, IT Standard, Guidelines, and Tools and Techniques for Audit and Assurance and Control Professionals. USA.

[7] Azizah, Noor. 2017. Audit Sistem Informasi Menggunakan *Framework* Cobit 4.1 Pada *E-Learning* Unisnu Jepara. Jurnal SIMETRIS, Vol 8 No 1 April 2017

[8] COBIT Steering Committee and the IT Governance Institute. 2000. COBIT® 3rd Edition Framework. Audit Guidelines.

[9] Pusilkom UI, 2018, Program Training CISA Review Course Tahun 2018 (Online). pusilkom.ui.a.id/?p=522 Diakses 25 April 2018, pukul 02.30 WIB.
[10]ISACA, 2018, Maintaince Your CISA (Online). http://www.isaca.org/Certification/CISACertified-Information-Systems-Auditor/Pages/Maintain-Your-CISA.aspx# certication Diakses 25 April 2018, pukul 01.58 WIB.
[11] Republic of Indonesia. Keputusan Menteri Ketenagakerjaan No 48 Tahun 2015 tentang Penetapan Standar Kompetensi Kerja Nasional Indonesia Kategori Jasa Profesional, Ilmiah dan Teknis Golongan Pokok Kegiatan Kantor Pusat dan Konsultasi Manajemen Bidang Auditor Teknologi Informasi [Decree of the Minister of Employment no. 48/2015 on the Stipulation of Indonesian National Work Competency Standards (SKKNI) Professional, Scientific and Technical Services Category Basic Principles of Head Office Activities and Management Consultancy for Information Technology Auditor]. Jakarta: Indonesian Secretariat