Sarcouncil Journal of Public Administration and Management

ISSN(Online): 2945-3712

Volume- 01| Issue- 01| 2022

Review Article **Received:** 06-04-2022 | **Accepted:** 16-04-2022 | **Published:** 21-04-2022

Why is it Important for IT Auditors to know About the Legal Environtment of IS?

Sarmila Sarmawat, Laura Artania S. and Iskandar Muda
Universitas Sumatera Utara, Medan, Indonesia.

Abstract: By following an audit process that is in accordance with IS law regarding this matter, the audit process can be carried out continuously and continuously so that it can produce recommendations for the best solutions/alternatives to overcome related problems. Of course the auditor must know the law of SI. This is very important to do so that the auditor understands the audit processes that must be carried out to meet international standards.

Keywords: IT, Legal Environtment, Technology Audit.

INTRODUCTION

Financial scandals involving Enron and Arthur Andersen LLP, and others resulted in requests for new legislation to prevent, detect, and correct irregularities that occurred. In addition, technological developments in the networked environment have resulted in security and privacy issues which are one of interest to legal and technical experts but are also currently topics that impact virtually every user of information. The Internet has grown exponentially from government and educational computer links to a complex worldwide network that is exploited by the vast majority of computer-savvy terrorists between new users and certain people. However, breakthroughs in terms of technology, developments have increased with various new problems to be addressed, consisting of security and privacy. This issue is often of concern to IT audit and control specialists depending on the impact on the public and the organization itself. Current legislation and governance planning will online communities and, as long as governance is within the community network, will have a final impact on influencing practices.

LITERATURE REVIEW

Information technology audit is a form of supervision and control of the overall information technology infrastructure. This information technology audit can run in tandem with financial audits and internal audits, or with other similar monitoring and evaluation activities. At first this term was known as electronic data processing audit, and now information technology audit in general is the process of collecting and evaluating all information system activities within the company. Another term for information technology audit is computer audit, which is widely used to determine whether the company's information system assets have worked effectively and integratively in achieving organizational targets.

In practice, IT auditors collect sufficient evidence through various techniques including surveys, interviews, observation and review of documentation. One thing that is unique, the audit evidence taken by the auditor usually includes electronic evidence. Usually, IT auditors apply computer-aided auditing techniques, also known as CAAT (Computer Aided Auditing Technique). This technique is used to analyze data, such as sales transaction data, purchases, inventory activity transactions, customer activities, and others.

The purpose of the Information Technology Audit is to evaluate the system's internal control design and effectiveness. Not limited to efficiency and security of protocols, development processes, and IT governance. The installation of controls is very necessary, but there needs to be adequate security protocols so that there are no security breaches. In an Information Systems (IS) environment, an audit is an examination of information systems, inputs, outputs, and processing. The main function of this IT audit is to evaluate the system to maintain the security of the organization's data. IT audit aims to evaluate and assess risks to safeguard valuable assets and establish methods to minimize these risks.

METHODS

A literature review is a description of studies relevant to the topic. Cybercrime continues day by day which requires new legislation and forms of billing to find resolution of certain problems, but needs new guidelines, policies and procedures to be developed. Where a good policy consists of:

***Corresponding Author:** Sarmila Sarmawat

1. Specification of required security features
2. Defining “reasonable expectations” of privacy as the issue of monitoring people's activities
3. Defines access rights and certain rights and protects assets from loss, confidentiality or damage through specification of user-accepted usage guides and also, providing guidance for external (network) communications
4. Defines responsibilities to all users
5. Build trust through an effective password policy
6. Recovery procedure specifications
7. Requires a form of threat to save
8. Provide users with supporting information

RESULT AND DISCUSSION

Result

Financial scandals involving Enron and Arthur Andersen LLP, and others resulted in requests for new legislation to prevent, detect, and correct irregularities that occurred. In addition, technological developments in the networked environment have resulted in security and privacy issues which are one of interest to legal and technical experts but are also currently topics that impact virtually every user of information. The Internet has grown exponentially from government and educational computer links to a complex global network that is shared by most of the terrorists who have computer skills between new users and certain people. However, breakthroughs in terms of technology, developments have increased with various new problems to be addressed, consisting of security and privacy. This issue is often of concern to IT audit and control specialists depending on the impact on the public and the organization itself. Current legislation and governance plans will affect online communities and, along with the role of government in community networks, will have a final impact on future business practices. IT auditors should be aware that the US federal government has passed a number of laws that are fair to issues of computer crime and IS security and privacy. Following are the laws governing computer crime. The computer attack that occurred in 1994 occurred due to an online computer attack by an irresponsible party. This includes access to networks by unauthorized parties and the exchange of information resulting in coercive attacks resulting in legal action to address cyber violence originating from e-mail. This happened because the attack was carried out on the computers of the US government at that time so that the level of data security and privacy became a form of threat at that time. The large number of internet users has the availability of the number of access to confidential information that is successfully accessed in certain networks. People's bank balances, social security figures, political information, medical records, etc. are accessed by people without the knowledge of the authorities. Theft in identification of information is a fast crime rate and use of the IS highway has a key component of other forms of crime. The privacy act occurred in 1974 where the requirements were carried out by federal agencies, consisting of:

Allows individuals to determine what records relate to data collected and developed by federal agencies.
Allows individuals to prevent records relating to a particular purpose from being used or available for certain other purposes in federal agency records without consistency.
Enables individuals to improve access to information relating to federal agency records and to correct or change them.
Requires federal agencies to collect, manage, and use personal information in actions that assess an action for legal needs and purposes, where information is current and more accurate, and protects certain information issues.

This is a part of certain legislation against violence against certain personal information in the online system. Communications Decency Act of 1995, This is more directed to indecent or patent rights to all forms of information technology through computer networks where everyone provides access or connections to or supports facilities, systems, or networks that are not under the control of violent actions by people. Health Insurance Portability and Accountability Act of 1996, This involves the privacy issue of medical-related organizations against the need to invest in some of the new technologies currently available in a given industry. Technology consisting of online certification, authentication, and biometric standards is needed to ensure that the person accessing it is the authorized party.

DISCUSSION

The audit process carried out in accordance with the IS legal environment is-

The responsibility of the auditor to publish the results of the audit to external parties of the organization. This is done so that external parties of the organization know the current and future conditions of the company.

Publisher: SARC Publisher

By knowing the IS policy, the auditor must readjust between the audit standards and the IS standards in each organization.

Establish procedures that the organization must follow so that the audit process can run smoothly and be accepted by the organization's management.

Checking the applications used in the organization,

And others.

CONCLUSSION

In carrying out TI audit and control activities over an organization, the Auditor as the actor organization, the Auditor as the actor conducting the audit process must know and understand the main areas/focuses in information systems law that applies universally/internationally. Without knowing the IS legal environtment, many IT Auditors carry out an information Technology evaluation process according to their knowledge and experience according to their respective perspectives or views on IT. If one auditor conducts an audit based on his views. The other auditors also conduct audits based on his views, then from an organization audied as objects will have more and more differences, otherwise the objects seen are the same. Without a standardization, all from of fraud that arise from the IT audit process are also many organizations so it is difficult to find a solution that fits the problems at hand. As a result, the audit process is considered troublesome. Therefore, as a good IT auditor, he must pay attention to and consider internationally applicable IT auditing standards and the information system laws that are followed to produce an effective and efficient audit process. So, the auditor can come up with recommendations that can be proposed as a strayegy to be further developed within the organiztion. It must also be able to maintain and protect the audit, privacy, and security of important information related to the audit so that there are no leaks produce results.

REFERENCE

1. Pathak, J. and Lind, M. “Audit Risk, Complex Technology, and Auditing Processes.” *EDPACS: The EDP Audit, Control, and Security Newsletter* 5 (2006): 1-9.
2. Senft, S. and Gallegos, F. “Information Technology Control and Audit." *Taylor & Francis Group, LLC* 3 (2009).
3. Pengertian Audit IT, diakses pada (https://itgid.org/it-audit/)
4. Tujuan Audit, diakses pada (https://www.dictio.id/t/apa-yang-dimaksud-dengan-audit-teknologi-informasi/15065/2)
5. Sikka, Prem. "Audit policy making in the UK: The case of ‘the auditor's considerations in respect of going concern’." *European accounting review* 1.2 (1992): 349-392.
6. Cangemi, M. P. "Views on internal audit, internal controls, and internal audit’s use of technology." *EDPACS* 53.1 (2016): 1-9.

Source of support: Nil; **Conflict of interest:** Nil.

Cite this article as:

Sarmawat, S., Laura, A.S and Muda, I. "Why is it Important for IT Auditors to know About the Legal Environtment of IS?" *Sarcouncil Journal of Public Administration and Management* 1.1 (2022): pp 12-14.