

The Effect Of IT Audit On Security Incidents

Armend Salihu, Xhemile Berisha - Hoti

Abstract: In this paper we present the effect of implementing IT Audit recommendations on organizations regarding the security incidents. From the data collected, we noted that with the implementation of IT Audit recommendations the security incidents are reduced. From the interviews we have seen that the IT Audit function is considered very important role in the prevention of the organization from security incidents and other cyber-attacks.

Index Terms: IT Audit, Internal Audit, Security Incidents.

1. INTRODUCTION

INFORMATION technology has become a reality that we need to coexist with. It has become a part of all scientific and application areas in all scientific and non-scientific fields and, due to its privileges in the realization of accounting, auditing and control objectives generally, its shadow over finance applications in general and accounting applications in particular. The role of information technology is responsibility for designing, implementing and keeping many of the controls over the business procedures of the organization. Information Technology plays a critical role in the collection, processing and storage of information summarized and recorded in financial statements [1]. Many organizations, which are increasingly dependent on Information Technology, are becoming progressively popular every day with such components as fully embedded data and electronic documents management. In terms of operational efficiency, cost savings and reducing human mistakes, Information Technology increases the accuracy and speed of transaction processing, and can even produce competitive advantages for numerous organizations. The risk associated with Information Technology on the other hand is numerous including [2] [3] [4] [5] [6]:

- Loss of computer assets;
- Erroneous recording;
- Increasing fraud risk;
- Competitive disadvantages if the wrong IT is chosen;
- Loss or theft of data;
- Violation of privacy; and
- Disruption to businesses.

For the last 20 years, significant changes in information technologies that have altered the nature of the internal control environment and the audit have led to the IT revolution that has inevitably transformed every aspect of our lives. Changes in traditional decision making have stimulated the need for timely, relevant, value-added, consistent and precise data and in turn have enhanced dependence on IT [7]. In latest years, the audit of information technology has become an increasing problem. The enhanced social and organizational function of information technology has boosted the requirement for an IT audit.

A growing need for executives to verify and secure processes of value generation in both private and public sectors and the complexity of information technology architecture and

infrastructures requires an increased awareness and an understanding of corporate governance in general and of IT governance in particular. IT governance is defined by the Information Technology Governance Institute as "leadership, organizational and processes which ensure that the IT of the company maintains and expands the strategies and objectives of the organization" [8]. In order to promote appropriate conduct using of IT, the IT governance may also be described as setting decision rights or accountability frameworks [9]. The most significant aspect for the organization's survival and success is the effectiveness of Information Technology governance. The IT audit is the method for collection and evaluation of evidence on the basis of which the performance of IT systems can be assessed, in other words whether the role of the information systems is to preserve the property and preserve the integrity of the data. There is also a need to determine if the Information Systems can achieve enterprise goals in an efficient and effective way and whether system resources are used. Today's IT audit reflects a contemporary and consultative role, "the right hand," which helps IT management [10]. Cannon and Crowe have stated that many of the internal controls over financial data are incorporated in IT-writing, implementing and maintaining computer programs, processes and procedures. Organization assets and liabilities can therefore be transmitted through computerized procedures without human intervention. In computer procedures that reside within external organizations, securities operations, material purchases and wire transfers are regularly launched and consummated. The degree to which human activity is automated may be limited to promulgating policies, rules and evaluating results. It is also argued that internal auditors are struggling to maintain their identity and purpose as the organizations they audit undergo radical changes. The dismantling of hierarchical control and control systems are total management of quality, reengineering of company processes, globalization and self-managed teams. Advances in IT are making control processes constantly obsolete and seriously question the "value" of traditional internal audit [11]. As IT changes take place faster, the auditors need to maintain up with new technology modifications and their impact on the information handling scheme of their customers as well as their audit processes [12]. Internal control for all divisions at any facility, whether products or services is a scientific database. Furthermore, there were some risks associated with the use of contemporary technology in penetrating and altering the information from inside and outside the facility. This technological utilization has also been supported by merits or possibilities that can be invested in achieving the strategic objectives of a particular institution. The update of internal control effectiveness needs secure technology that helps to keep financial and non-financial information confidential.

• Armend Salihu, South East European University, Ilindenbska n.335, 1200 Tetovo, Macedonia. E-mail: ar.salihu@gmail.com

• Xhemile Berisha - Hoti, Universiteti i Prishtines, Faculty of Economy, Rr. "Agim Ramadani" p.n., 10 000, Pristine, Kosovo. E-mail: xhemileberisha@gmail.com

2. LITERATURE REVIEW

There are rising costs or errors, for example, which could lead to a company's competitive position or even its mere presence, because the information system is inadequately formed or is of low quality. That is why all its objectives, activities, like: data collection; processing and storage; information preparation; evaluation; management and distribution, and all elements like: hardware; software; data-ware or net-ware, have to be covered in order for information system control and audit functions to be formed. [13]. There are generally seven significant factors to establish the control and audit function of the information system [14] [15]:

1. Consequences of loss of data and organization's expenses;
2. The possibility or expenses of making mistaken choices because of inaccurate data or poor information systems;
3. Information equipment costs misuse because the data or computer system controls do not exist or have inefficient results;
4. Value of each component of the information system (hardware, software, data ware and net ware);
5. Costs of PC and different equipment errors;
6. Need to maintain data protection;
7. Need to improve information equipment in a controlled way.

In the private and public sectors, the frequent use of information technology has created many new difficulties as well as possibilities for security, confidentiality, reliability and data integrity. Therefore, new audit processes are required if the audits are to be implemented successfully [16]. Technology, as being identified by Porter [17], is one of the five forces that drive industry competition. Since the functioning of the information system will be a decisive part of the efficiency, effectiveness and success of all business operations, the problem of systematic supervision and audits needs to be addressed. Information system auditing is an organizational role in which the functions, purposes and parts of the information system can be independently and objectively tested to provide evidence that can be regarded independently or provide a good basis for other auditing types. The purpose of the information system audit is to conduct a systematic, comprehensive and detailed examination of information system controls to warn of possible mistakes and risks and therefore to assess the quality of the information system of the company [13]. In latest years, the effect of IT on businesses has increased exponentially, changing the audit process and creating auditors with possibilities and difficulties. In reaction to environmental changes, the audit profession advances quickly [18]. With IT change more rapidly, auditors need to follow up on evolving technological modifications and their effect on the information handling system of their organizations and their own auditing processes [12]. As information technology use becomes more complicated in organizations, auditors must employ technologies, comprehend them and be able to efficiently audit procedures and use them as an audit tool [19]. Organizations use best practice frameworks to support progress to enhance IT management in line with regulatory requirements. One of these IT governance frameworks is COBIT, which provides guidance as to what an organization can do with regard to process and operational control activities, measures and documentation. COBIT is the world wide-

ranging accepted standard for IT Governance, information technology and related IT processes which specifies IT governance areas and individual controls [10]. The latest COBIT version is COBIT 2019 [20]. The IT Control service consists of the testing of computers, networks, software and office equipment. The IT audit enables issues and weaknesses to be resolved effectively. Further infrastructure development planning is needed [14]. The function of Information Technology is presently to ensure the audit efficiency in terms of its accuracy, timeliness and integrity and thus strengthen the legitimacy of the financial data submitted to a broad spectrum of customers [21]. IT Auditing is a collection and evaluation method aimed at assessing whether a computer system is intended to preserve data integrity, protect property, efficiently achieve organizational objectives and efficiently use of resources [22]. Many organizations understand after some time that their IT portfolio contains a number of costly technologies. Each of them only includes a part of the objectives of the organization. These techniques are not easy to integrate and handle. The IT audit results in the following fields to identify issues:

- Compliance of IT systems with corporate strategy;
- IT architecture status and deviations from the standards required;
- The state of the systems used by companies depends on: functionality, reliability, usability, technology, innovation, system documentation and the overall performance of services.

Simultaneously the objective of a new audit guidance is to improve financial, compliance and performance audit outcomes. IT audit may evaluate the environment of the information systems of various agencies and businesses, which affects economic data and accounts of the organization for the proper reliability of reflection. The audit will enable the amount of compliance with the regulatory legislation by IT system security to be evaluated. Moreover the IT system operational efficiency, effectiveness and productivity is provided by an information technology audit. The e-governance associated risks are developed by the IT auditing. In specific, the risks have shifted from the document to the Slate Electronic Systems while increasing possibilities for fraud, robbery, distortion and distribution. The new auditing strategy identifies information security, data integrity, and fraud risks in information systems and offers the appropriate prevention suggestions, as well as enhancing the scope of the audit using this innovative audit strategy [23]. The effects of the risk to inputs and outputs and the activities of the accounting system have been recognized on the effectiveness of Jordanian commercial bank accounting control, administrative control and internal control. As a tool for collecting preliminary information, a questionnaire was used to distribute it to internal auditors and financial executives. Statistical techniques like standard deviation, means, Cronbach's Alpha test and one sample t-test were also used. The most significant suggestions in the research are that the parts of the accounting system must be examined as one unit in relation to inputs, outputs, feedback or the activities of the accounting system in order to determine its effect on internal control effectiveness, and the need for scientific meetings focused on the general risk to the processes of internal control effectiveness [24]. Bo-Hayek has demonstrated the impact of an effective accounting system on the Algerian General Petroleum Company in achieving the

necessary efficiency of internal controls. The research was based on a questionnaire to the study population consisting of financial executives, internal auditors and internal control staff. There were also use of arithmetic means, frequencies and percentages. It has been shown that the structure of the organization, by the presence of a data system which truly represents economic occurrences, measures the authority of its internal control system. In order to achieve internal control effectiveness, the business can also profit from the utilization of the electronic work environment. One of the recommendations is the need to apply the primary and secondary qualitative characteristics to ensure high credibility of accountable information, and the request to recognize the role of human resources as an institutional investment and enhance its skills and qualification to the level needed to achieve internal control [25]. The strength of internal control systems has been recognized and evaluated by Al-Sawaf to reduce risks during daily operations at the banks. The purpose of the review was also to ensure the significant role of internal control and auditing in protecting and continuing banks by determining the effect on the operational risk of internal controls and auditing. The research was based on the distribution of questionnaires by the research sampling participants represented by internal control staff in the banks, and some outcomes were obtained which revealed the agreement of the majority of the participants on the importance of the internal control and auditing in order to prevent operating risks. This demonstrates in turn the function of internal control and auditing in the management of risk. The need to define the control risks for future management and the need to issue special legislation to cope with the special risks posed by the banks [26]. Alshaibi has demonstrated the significance of internal control system in the audit process to adapt to the rearrangements of IT equipment and their consideration of the credibility of the financial statements. The study population was comprised of the Libyan banks belonging to four banks of the state. A questionnaire was developed so that the variables of the study could be observed and circulated in those banks on the IT and internal control departments. The research used the arithmetic mean, the standard deviation and the one sample t-test. The growth of the Libyan banks has shown a decent amount of adaptation of internal control mechanisms to the IT needs. The most significant suggestions of the research are the need to establish or appoint control bodies to create and enhance the legitimacy of their financial statements, which provide for the necessary legislation [27]. The impact of input risks on accounting control, administrative control, and internal control was identified by AL-Sharairi, Al-Hosban and Thnaibat. The study data were obtained through the questionnaire. There were internal auditors at commercial banks in the research group. The methods used were statistical ones like: arithmetic mean, standard deviations and the Cronbach's Alpha test. The effect on administrative control, accounting and internal controls of the risks of accounting information systems has been shown. It is suggested that all of the data in the accounting system be documented and that employees be trained to decrease the risk in particular for accounting systems [28]. The role of the internal auditor for computer systems technology has been recognized by Alhosban and Al-Sharairi. In addition to the auditor's role in the physical components of computer networks and maintenance, the objectives were to determine the role of the computer networks installed for the first time. A total of 101 questionnaires had been circulated and 89 questionnaires had

been selected for statistical analysis, including internal auditors at Islamic banks or financial institutions. For testing the research hypotheses, a single sample test was used. For the internal consistency of the research sample the arithmetic mean and Cronbach's alpha test were used. The main findings of the research are showing whether computer networks have an effect on the internal audit work environment both when the computer is first installed and when physical parts of computer networks are provided. [29]. The following fundamental IT audit types can be combined to summarize the literature [23]:

- General IT audit - The most efficient technique for detecting issues in all key IT infrastructure stations is a general IT audit. It provides an opportunity to evaluate the state of the IT systems and eliminate a specific system for eliminating the problems that already exist, with the highest protection and conservation of the investments being carried out - it means that the plan won't be called to make sure that "everything must be destroyed and rebuilt".
- Hardware audit – The measurement complex comes from the study we receive on the quantitative and qualitative features of IT infrastructure hardware of the organization.
- Software audit – It is the evaluation of the organization's software products for evaluating effectiveness, updates and the degree of license purity. The assessment of software products used in the organization, also preventing license breaches and associated adverse effects, allows the management of organizations to make maximal use in the use of software products.
- Security audit – This is the analysis in line with international standards of information security systems. The purpose of the audit is to improve data protection and minimize risk related to the operation of an information system. Analyzing the IT infrastructure parameters such as human factor impact, safety, system access, private transfers and sustainability storage technologies can achieve this objective.

IT auditing is necessary if the business needs the computer infrastructure to be implemented or upgraded or if employees change and restructuring, even when the technical resources efficiently are actually utilized. The separate IT audit inquiry substantially reduces operating costs for infrastructure.

3. METHODOLOGY AND RESULTS

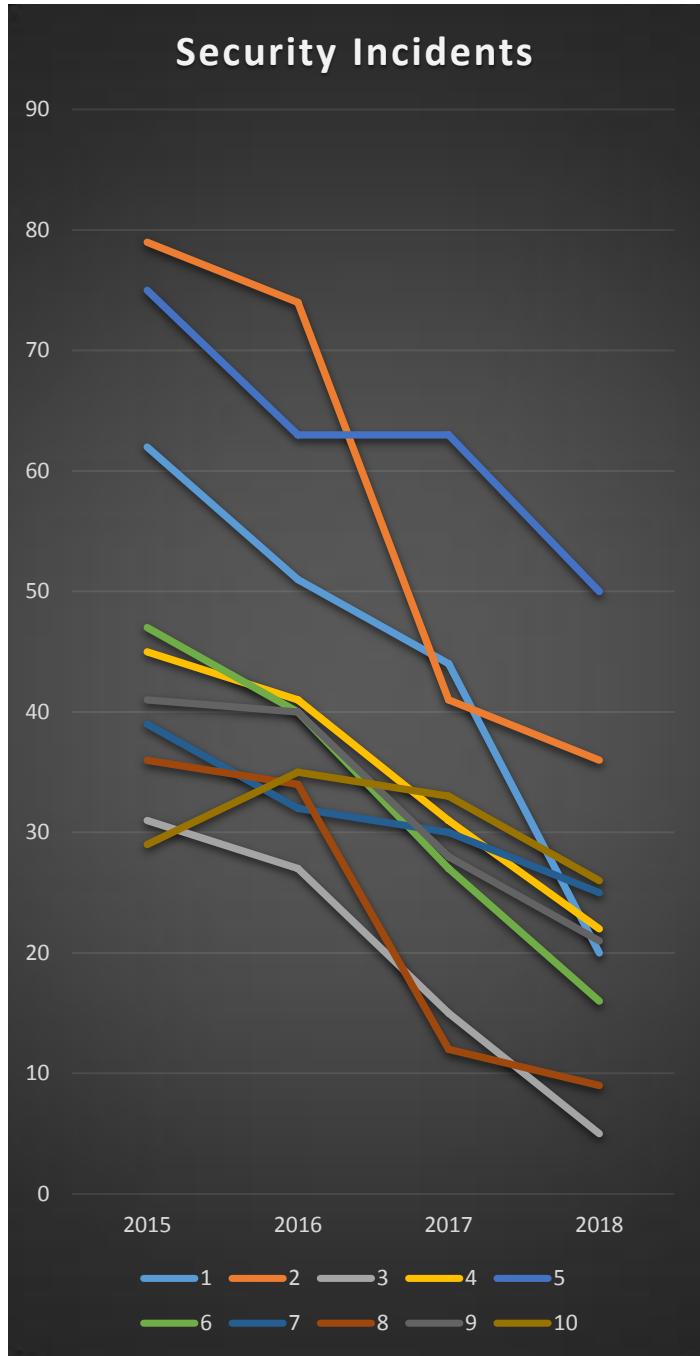
In this paper we evaluated the impact of IT auditing on security incidents. In order to realize the effect of implementing recommendations in the field of information technology in reducing security incidents, we have looked the total number of the given recommendations for the four year period starting from 2015 to 2018, we have also looked at the total number of implemented recommendations, where we have found that almost all of the recommendations given in the field of information systems have been implemented by organizations. Whereas to establish a connection that the implementation of recommendations in the field of information technology has an impact on the reduction of security incidents, we have taken the total number of security incidents from which we have noticed that every year there has been a decrease in number of security incidents.

TABLE 1 DETAILS OF GIVEN AND IMPLEMENTED RECOMMENDATION AND SECURITY INCIDENTS

Year	Organization	Given Recommendation	Implemented Recommendation	External IT Audit Recommendation	Security Incidents
2015	1	28	28	18	62
	2	N/A	N/A	29	79
	3	21	21	10	31
	4	29	28	21	45
	5	32	32	26	75
	6	N/A	N/A	22	47
	7	27	27	13	39
	8	12	12	19	36
	9	19	19	15	41
	10	33	30	N/A	29
2016	1	17	17	12	51
	2	11	6	26	74
	3	19	19	6	27
	4	25	25	15	41
	5	29	29	5	63
	6	27	27	20	40
	7	29	29	17	32
	8	18	18	9	34
	9	17	16	15	40
	10	29	29	N/A	35
2017	1	22	22	14	44
	2	23	23	20	41
	3	12	12	9	15
	4	21	20	11	31
	5	22	22	8	61
	6	26	26	N/A	27
	7	25	22	15	30
	8	11	11	12	12
	9	21	21	13	28
	10	19	19	N/A	33
2018	1	15	14	51	20
	2	18	18	N/A	36
	3	9	9	27	5
	4	12	10	41	22
	5	23	23	63	50
	6	21	21	N/A	16
	7	31	26	17	25
	8	10	10	34	9
	9	18	16	12	21
	10	22	22	N/A	26

In this research we have gathered the necessary data from 10 different organizations. Details of the data are presented in Table 1, while Figure 1 shows the graphical representation of security incidents from which it is also seen that there is a decrease in security incidents from year to year.

FIGURE 1: NUMBER OF SECURITY INCIDENTS OVER THE YEARS



From the presented data it can be seen that the implementation of recommendations has positively impacted on the reduction of security incidents and has had a positive effect on improving the organization system and information security. For this research, we conducted interviews/questionnaires with the organizations' managers, as well as heads of information technology units, information security officers and IT auditors. Seven different questions

regarding the impact of IT Audit on these interviews were presented:

- When asked whether the internal IT audit adds value, we have received a positive response from all the interviewed parties.
- When asked whether the implementation of internal audit recommendations in the Information Technology field has affected the organization's protection from security incidents, we have received a positive response from all interviewed parties.
- When asked whether internal IT audit has impacted on improving IT business processes, we received a positive response from all respondents, with little concern from IT managers that some additional control procedures could affect human resources.
- When asked whether the areas covered by the IT Auditor who did not detect any deficiencies, whether there were any security incidents, we received a negative response from all interviewed parties, where in the areas addressed by the IT Auditor there were no cyber-attacks and security incidents identified.
- When asked whether the implementation of IT Auditor's recommendations to reduce security incidents had an impact, we received a positive response from all interviewed parties. Where implementation of the recommendations of the internal auditor in the IT field, there was a very high impact on reducing security incidents.
- When asked if the findings identified by the external auditor of IT, the same were previously identified by the internal auditor of IT, we got the answer that all important issues are identified by the internal auditor of IT on time.
- While the question as to which audits are most effective, those of the IT internal auditor or external auditor, the organizations' managers, the heads of IT units and the information security officers, we had responses that internal audits are more effective, and from this question are excluded internal IT auditors.

4. CONCLUSION AND DISCUSSION

We have noticed in a literature review that IT Audit is a significant position within the organization and that it is able to assist decrease security incidents and boost the efficiency of IT units. COBIT is one of the frameworks for IT governance and gives guidance on how procedures and activities in an organization can be controlled, measured and documented. The latest COBIT version is COBIT 2019. In general, seven significant reasons have been recognized to establish an information system control and an audit function: Consequences of loss of data and organization's expenses; The possibility or expenses of making mistaken choices because of inaccurate data or poor information systems; Information equipment costs misuse because the data or computer system controls do not exist or have inefficient results; Value of each component of the information system (hardware, software, data ware and net ware); Costs of PC and different equipment errors; Need to maintain data protection; Need to improve information equipment in a controlled way. The following types of IT audit functions are summarized: General IT audit, Hardware audit, Software audit, Security audit. From the data gathered and interviews, we have seen that the number of security incidents is decreased with the

implementation of IT Audit recommendation. From the questionnaire, we have seen that the IT Audit function is very important role within the organization and is strongly related to the security incidents and organizations' system prevention.

REFERENCES

- [1] D. M. Cannon and G. A. Crowe, "SOA Compliance: Will IT Sabotage Your Efforts?," *The Journal of Corporate Accounting and Finance*, vol. 15, no. 5, pp. 31-37, 2004.
- [2] J. Warren, L. Edelson, X. Parker and R. Thrun, *Handbook of IT Auditing*, New York: Warren, Gorham & Lamont, 1998.
- [3] U. Gelinas, S. Sutton and A. Oran, *Accounting Information Systems*, Ohio: South-Western College Publishing, 1999.
- [4] D. R. Hermanson, M. C. Hill and D. M. Ivancevich, "Information Technology-Related Activities of Internal Auditors," *Journal of Information Systems*, vol. 14, no. 1, pp. 39-53, 2000.
- [5] B. L. Hadden, F. T. DeZoort and D. R. Hermanson, "IT Risk Oversight: The Roles of Audit Committees, Internal Auditors, and External Auditors," *Internal Auditing*, vol. 18, no. 6, pp. 28-31, 2003.
- [6] A. Abu-Musa, "Exploring Perceived Threats of CAIS in Developing Countries: The Case of Saudi Arabia," *Managerial Auditing Journal*, vol. 21, no. 4, pp. 487-507, 2006.
- [7] M. Kayrak, "Information Technology Audit in the Context of Information Criteria," *Journal of Turkish Court of Accounts*, pp. 143-167, 2012.
- [8] IT-Governance-Institute, *Board Briefing on IT Governance*, 2nd Edition, USA: IT Governance Institute, 2003.
- [9] P. Weill and J. W. Ross, *IT Governance – How Top Performers Manage IT Decision Rights for Superior Results*, Harvard Business School Press, 2004.
- [10] D. Radonovic, T. Radonovic, L. Dubravka and M. Sarac, "IT audit in accordance with COBIT standard," in Conference: MIPRO, 2010 Proceedings of the 33rd International Convention, IEEE, 2010.
- [11] J. D. Tongren, "Co Active audit: The enhancement audit model," *Managerial Finance*, vol. 23, no. 12, pp. 44-51, 1997.
- [12] Z. Rezaee and A. Reinstein, "The Impact of Emerging Information Technology on Auditing," *Managerial Auditing Journal*, vol. 18, no. 2, pp. 465-471, 1998.
- [13] M. Spremić, "Managing IT Risks by implementing Information System Audit Function: Case of Croatian Large Companies," in 3rd INTERNATIONAL WORKSHOP IN WIRELESS SECURITY TECHNOLOGIES PROCEEDINGS, 2005.
- [14] R. Weber, *Information systems control and audit*, Prentice Hall, 1999.
- [15] Z. Panian, *Kontrola i revizija informacijskih sustava*, 2001.
- [16] M. Kayrak, *Information Technology Audit and the Practice of the Turkish Court of Accounts*, 2014.
- [17] M. E. Porter, *Competitive Advantage*, New York: Free Press, 1988.
- [18] I. Solomon and K. Trotman, "Experimental judgment and decision research in auditing: The first 25 years of AOS," *Accounting, Organizations and Society*, vol. 28, pp. 395-412, 2003.
- [19] S. Hass, M. J. Abdolmohammad and P. Burnaby, "The America's literature review on internal auditing," *Managerial Auditing Journal*, vol. 21, no. 8, pp. 835-844, 2006.
- [20] ISACA, *COBIT® 2019 FRAMEWORK: INTRODUCTION & METHODOLOGY*, USA: ISACA, 2019.
- [21] K. Omoteso, *Audit Effectiveness: Meeting the IT Challenge*, Brookfield: Gower Publishing Co., 2013.
- [22] F. B. Veerankutty, "INFORMATION TECHNOLOGY (IT) RELATED AUDITING IN MALAYSIAN PUBLIC SECTOR: An Empirical Study of National Audit Department of Malaysia," 2010.
- [23] T. Beridze, "Information Technology Audit in Georgia," *European Scientific Journal*, vol. 13, no. 25, pp. 72-93, 2017.
- [24] D. Y. Abu, "The impact of accounting information systems on the effectiveness of the internal control system in Jordanian Commercial Banks," University of Jordan, Jordan, 2017.
- [25] A. Bo-Hayek, "The role of the accounting information system in the effectiveness of internal control in oil companies in Algeria," University of Qasidi Marhaba, Algeria, 2015.
- [26] M. Al-Sawaf, "The effect of internal control on the sizing of operational risks in commercial banks," *University of Mosul Journal Iraq*, 2011.
- [27] M. Alshaibi, "Adapting internal control system with a use of IT and its effect on reliability of financial statements," Jordan, Amman: Middle East University, 2011.
- [28] M. AL-Sharairi, A. Al-Hosban, and H. Thnaibat, "The impact of the risks of the input of accounting information systems on managerial control, accounting control and internal control in commercial banks in Jordan," *International Journal of Business and Management*, vol. 13, no. 2, pp. 96-107, 2018.
- [29] A. Alhosban and M. Al-Sharairi, "Role of internal auditor in dealing with computer networks technology - Applied study in Islamic banks in Jordan," *International Business Research*, vol. 10, no. 6, pp. 259-269, 2017.