Cloud Computing Auditing

Roadmap and Process

Mohammad Moghadasi, Dr. Seyed Majid Mousavi, Dr. Gábor Fazekas
Department of Informatics, University of Debrecen, Hungary

***Abstract*—Cloud Computing is a new form of IT system and infrastructure outsourcing as an alternative to traditional IT Outsourcing (ITO). Hence, migration to cloud computing is rapidly growing among organizations. Adopting this technology brings numerous positive aspects, although imposing different risks and concerns to organization. An organization which officially deputes its cloud computing services to outside (offshore or inshore) providers and implies that it outsources its functions and process of its IT to external BPO services providers. Therefore, customers of cloud must evaluate and manage the IT infrastructure construction and the organization's IT control environment of BPO vendors [25]. Since cloud is an internet-based technology, cloud auditing would be very critical and challengeable in such an environment. This paper focuses on practices related to auditing processes, methods, techniques, standards and frameworks in cloud computing environments.**

Keywords—Cloud computing; cloud auditing; IT outsourcing

I. Introduction

Outsourcing IT operations is not a new concept. Recently, Cloud computing is a new concept in the outsourcing IT operations as an adopted paradigm for delivering IT services over the Internet by organizations. Maximum utilization of hardware and software by sharing resources through virtualization, elastically, flexibility and decreasing capital and operational expenditures (CAPEX and OPEX) has made popular this IT paradigm. Supporting thousands of business needs, Simplify and streamline enterprise collaboration, cost management, availability, and scalability are only a few of countless motivations for organizations to adopt cloud computing. This new technology also brings risks and concerns to organization. The number of IT outsource providers in cloud recently has increased and this increment has brought large number of risks to the scene. As well as the providers, IT outsourcing risks are considerably increased, these risks are applied and enforced all over the life cycle of cloud computing and its services, either an organization is already implemented cloud services and solutions within its environments or planning on becoming a cloud-based company or an affiliated organization [1]. This paper contributes to provide a comprehensive perspective in auditing processes, different approaches and frameworks, and key concepts in cloud computing environments.

According to SOX section 302 [2], Chief Financial Officer (CFO) and Chief Executive Officer (CEO) support the credibility of their corporation and are responsible for the accuracy of financial reports of their company annually and quarterly. Even if these business reports and relevant data exist in different locations, units, teams, departments, business sites, data centers and or in different cities or countries [35]. Thus, for organizations, it is important that the IT operations in the cloud comply with applicable legislation and SLAs (Service Level Agreement).

As cloud computing is a new orientation in IT and business processing outsourcing, organizations would make good use of this technology in their business procedures [26]. The importance of IT auditing and especially cloud computing auditing is an essential effort to ensure the proper functioning processes of an organization's IT systems, management, operations and related processes, to avoid fraudulent, in order to have comprehensive and accurate financial view of their business. Internal auditing is a crucial component of any organizational processes; thus, being a strategic collaborator to an organization is not the only essential element but performing ordinary quality assurance is also crucial in cloud-based organizations. As well as enhancing the organizations' productivity and efficacy in the improvement of their IT processes throughout these activities. [3,4 and 34]. Hence, this paper aims to provide a contribution to the understanding of different aspects in cloud auditing [33], its risks and benefits in cloud environments, in order to shed light on the cloud computing audit practices. In this paper, we address different cloud auditing practices related to processes, techniques, test steps, standards and frameworks with the purpose of answering the following questions: 1) How to maximize the value of the IT audit function? 2) What are specific components and key controls which might be necessary for cloud environment auditing? 3) How to determine appropriate cloud auditing process? 4) Which frameworks and standards are recommended to do a cloud audit?

The present paper is structured according to the followings: The forthcoming section differentiates between IT outsourcing and cloud computing [25]. The implication and importance of cloud auditing are explained in section three. After that, in section four, cloud auditing approaches and techniques are discussed. Test steps and key controls come in section five. Sixth section points out cloud auditing standards and frameworks [25]. And at last as a final result of this paper a conclusion is presented in section eight.

II. IT Outsourcing and Cloud Computing

A. IT Outsourcing

Most of the times, impossibility of conducting all aspect of affairs, business process or being temporarily some processes justify hiring external required resources and professionals to perform operations in organization [5]. Utilization of external required resources to conduct a specific business processes, is

usually a strategic decision based on a desire to reduce costs and to allow a company to focus on its core competencies. IT outsourcing is a subset of business process outsourcing (BPO) [6]. The main implication of IT outsourcing is, moving all or parochial of IT functions to an external company. Two main objectives of IT outsourcing for most of organizations are: lack of adequate resources and cost reduction strategies. IT outsourcing has different models for organization which is chosen based on organization needs and strategy, but adopting a model is not always easy. Types of IT outsourcing models are: Application Service Provider (ASP), Application Develop & Maintenance (ADM), IT Infrastructure Outsourcing (ITO), and IT Services [25].

B. Cloud Computing

Cloud Computing facilitates and empowers the IT process outsourcing by which the approachability of IT-related services and resources such as delivered-platforms, hardware, software on the internet as service for a basis charge monthly, quarterly or annually [7]. National Institute of Standards and Technology also known as the NIST has the following definition for Cloud Computing [8]:

''Model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [8]. The opportunity to purchase and centralize IT support/services by using external infrastructure and another organization's resources to provide the mentioned services is an outsourcing decision in cloud computing [6,7]. The Cloud Computing technology is processed through three layers (IaaS, PaaS, SaaS), relying on such computing concepts as virtualization, grid and distributed computing and Service Oriented Architectures (SOA) [9,25]. The main concepts which are listed by the cloud community and the NIST organization include hosting, roles, deployment and service models and necessary and important specification [10].

There are different perspectives on how IT process outsourcing differs from Cloud Computing. In case of Cloud Computing, an application is originated in the cloud itself by default, whereas with IT outsourcing, a specific function is relocated from its original geographic jurisdiction, enterprise, site or department [11]. Network-based applications, length of contract, saleable services and requests, flexible self-service interface and shared resources, in order to achieve maximum density, are the other major differences between IT outsourcing and cloud computing.

Cloud computing adoption and its popularity among companies are rapidly growing because of both economic and technical aspect. With respect to its positive aspects, Cloud Computing risks should be considered and mitigated as well. Cloud computing risks affect quality of service (QoS) to customers. The major cloud environment risks have been reported in control access management, vendor management, regulatory compliance, data privacy, and operational process. In order to overcome such risks continuous audit is needed in cloud environment.

III. Cloud Auditing

IT outsourcing life cycle consists of several phases, and each phase may encounter uncertainties and risks. Therefore, in order to risk quality control and identification of IT outsourcing, a systematic auditing is required to be applied to the entire life cycle of IT process outsourcing.

Cloud computing appearance is a novel form of IT system and infrastructure outsourcing as an alternative to traditional IT outsourcing. According to technical and economic perspectives, Cloud Computing has numerous advantages pushing for its development and quick assumption [13]. An organization which officially deputes its cloud computing services to external providers and points out that it outsources the process of its IT and functions to external ITO services providers [25]. According to SOX regulations, management's responsibility in sustaining efficient internal control over financial reporting will not be affected or reduced by using a service organization [2]. Thus, Customers of cloud computing execute a consecutive and successive evaluation over the IT control and provider environment [25].

Regardless numerous advantages, cloud computing has been associated with numbers of risks and concerns, which attracted IT auditor's attention. Auditing's main and primary implication is; "an independent and autonomous experiment of an organization's management assertions declared by an external sanctioning body that must follow a set of guidelines and standards" [14, 25].

Thus, IT auditors must have complete comprehension of cloud computing and auditing methods to assess, evaluate and assurance of regulatory compliance and SLAs (Service Level Agreements). The auditing work is much different and more complicated than regular IT auditing, and as a result cloud computing involves external vendor's help or partner's support to control [12,15,16,19 and 25]. The cloud audit can be internal or external as regular IT audit. Internal audit is performed by inside auditors to analyze and assess the data and processes for improving organization's effectiveness and efficiency. External audit is conducted by auditing firms or expert auditors. Organizations are obliged to comply with mandatory audit to demonstrate regulatory compliance and voluntary audits include processes, practices, internal controls and the independent validation or quality assurance and those associated with certification [17]. A major asset in corporate governance and financial reporting and its public confidence improvement is efficacious auditing function if this effective action includes following elements; approved audit-charter and audit-committee existence, unlimited scope, stakeholder support, un-restricted access, sufficient staff, professional-audit standards, competent leadership, adequate funding, formal mandate and organizational independence [18,20].

Providing an assurance engagement between consumers and cloud services provider for cloud auditing is a major motivation to raise the measurement of criteria against cloud services and the confidence of cloud consumers. Cloud auditing is a major tool to help organization's board and management, as an evaluation function to identify risks [26,29]. The auditing in cloud environment may be applied on specific sector such as: entity-levels, application systems,

security, application systems, data center, virtualized environments and web application (IT governance and customer relationship management (CRM) and enterprise resources planning (ERP)) [11,26].

IV. Cloud Auditing Techniques and Process

The auditing process is a consolidation of different ISA (International Standards on Auditing) and audit methodology which can be performed by internal or external auditors. It is important for auditor to consider that auditing is a continuous process and performed at various stages. It is also noteworthy for auditor to note that some stages can be combined with other stages or may need to return and rethink on previous completed stages.

The main purpose of IT auditing is to provide an independent opinion to ensure whether IT operations and governance comply with standards and SLAs. Substantive testing phase alongside Tests of controls as well as planning of an audit are the three main phases that can be performed by IT-audit process [12,21 and 25].

- *Audit planning phase*: In the first phase, planning phase, auditor must gain deep comprehension of the nature of business. Collecting and analyzing important information (such as IT operations, internal controls and risks) must be performed by auditor. During this phase auditor comprehend organization's policies, practices and structure. Practical approaches to gain evidence are: reviewing documentation and application, interview (management, employees), questionnaires. The three major stages of audit planning phase are introduced as followings: (1) procedures of substantive examination and scheme examination of controls, (2) organization's structure, course, terms and conditions review, (3) application and comprehensive control review [12,25].
- *Control examination phase*: In second phase auditor performs different tests to ensure internal control compliance over IT operational activities. During this phase, the auditor assesses quality of controls. The stages of this phase are: (1) control stage of specifying the reliance degree, (2) executing examinations of controls, (3) test outcome evaluation [4,5,21 and 25].
- *Main substantial testing phase:* The third phase focuses on investigation of financial data. During this phase substantive tests are performed in data files by using appropriate audit tools and techniques. The three stages of this phase include: (1) executing main substantial tests, (2) report of result assessment and issuing report of auditor, (3) creating audit report [21].

Checking the quality of processes of an IT operational are the purposes an IT audit's, whether the objectives and targets of a company or establishment are met by their IT processes or not [5,25]. An independent and systematic test, by ISO describes a quality audit as; "to achieve an organization's targets, planned regulation and adjustments must be complied with results of relevant quality operations whether or not, effective implementation of these regulations is suitable" [30,36]. It is explicit that IT auditing and all related areas on cloud computing operations can be developed by the quality concepts (Merhout. J.W., Havelka. D) [14,36], amongst the 108 identified unique factors, and based on existence control, efficacy, factor determination and what or who a propounded framework of IT audit quality consisting of eight categories. These eight categories are described in Table 1.

TABLE I. Descriptions of IT Audit Quality Framework Categories (Merhout and Havelka)

Categories	***Description***
Factors of Audit team	Teamwork experience, communications and teamwork quality,
Audit methodology and processes factors	IT audit team follows particular practice and procedure,
Client-controlled organizational factors	Critical client partnerships during an audit's course, management's support and adequacy of documentation,
IT Audit-Controlled Organizational Factors	Business unit comprehension, client relationship with organization, allocating sufficient time for all of audit, leadership and IT organizational assessment and change ability,
Technical qualification factors of IT audit personnel	Personnel experience, risks understanding and weakness control project management,
Interpersonal and social factors of IT audit personnel	Enthusiasm, capability and willingness to change, communication proficiency, motivation and independence,
Organizational environment and enterprise environmental factors	Internal audit's reporting structure, recent audit numbers, corporate culture, financial resources and audit's value perception,
System and target process factors	System type and complexity, processing of manual versus automatic amount, system or process documentation level, clearly defined project scope

Additional value over the primary assurance objectives can be provided by IT audit activities [14,25]. Work of regular IT audit can be similar to the cloud computing audit work as long as effective auditing framework and risk assessment method are chosen and followed by cloud computing's IT auditors. [25]. There are two major IT audit processes: Risk-based IT audit and Value-added IT audit [14]. Thus, during the cloud audit, the audit team establishes auditing process on value-added audit or risk-based audit. Each process has a specific auditing domain.

C. Value-Added IT Audit

Value-added and quality are consumer-focused concepts in organizations, and a new trend to conduct IT auditing. Value-added IT focuses on the organization's IT operations and capabilities. Value-added audit is a proven method to assess effectiveness of an organization's operations (such as quality, business process, IT, etc.) that verifies compliance with policies and procedures. According to the IIA (Institute of Internal Auditors) [9,31], following scopes are covered by a quality audit: Business process efficiencies, Trade process and business control, Commerce risks, Quality and utilizable efficiency and effectiveness, Cost diminution situations, Corporate governance effectiveness and Waste deletion

opportunities [4,22,23], and also value-added auditing is defined as follows: "Internal auditing is designed to improve companies' operations and enhance relevant assurance values, since this activity is an independent, objective and consulting, and using this would facilitate organizations through the accomplishment of their objectives by bringing disciplined and systematic techniques to appraise and progress control, risk effectiveness management and governance methods" [14,25,36]. Some of value-added IT audit benefits are in Table 2.

TABLE II. VALUE-ADDED IT AUDIT SERVICES (MERHOUT AND HAVELKA)

1. Improved information technology governance by using proven return on investment in IT
2. Improved business process management or operational expediency and productivity through IT process and business progress reengineering by using audit documentation,
3. Improved risk mitigation through enhanced enterprise risk management (ERM) awareness by using audit observations,
4. Improved business continuousness and associated systems disaster recovery planning,
5. Improved systems development quality approach,
6. Increased trust development and organizational communication through facilitation among various stakeholders,

D. Risk-based IT Audit Process

An audit includes risk-based audit to focus effectively and expeditiously on the timing, nature and extension process in the mentioned scopes and to assure of having misstatement cause and its potential material in financial reports [23,25]. Internal audit can be accredited and empowered by risk-based audit to assure the board that whether or not risk management processes are complying effectively.

A risk-based IT audit identifies substantial IT threats and risks in IT operations area such as: risk assessment, security, data safety, IT governance, and systems development. Risk-based IT audit defines appropriate strategy for assessing IT operations and present proper solutions for risks mitigation. Even though IT function's quality and modality maintenance as well as value development is targeted by value-added IT audit but maximizing IT quality is the goal. [25].

V. CLOUD AUDITING: TEST STEPS AND KEY CONTROLS

Following objectives must be covered by the cloud audit as defined by ISACA [28]:

- Providing stakeholders with internal security policy and successful control process of the cloud computing service provider and productiveness evolution
- Providing an interface between the service provider and organization's client for identifying insufficiencies and inadequacies of internal control
- Providing an assessment criteria and report of capability and quality to audit stakeholders to be confident of the certification and accreditation of service provider and its internal controls

In addition to above objectives, the auditor must consider control access, authorization and trusted control frameworks, communications latency, data breach notification and international laws. A transferred system to the cloud or/and IT services support and reinforce business functions which must be contemplated and considered by the cloud auditor [3,32].

Cloud auditor must understand the associated risks, dealing with, and ability to develop an audit strategy and plan. Since cloud computing architectures consist of different models, services and components from other form of IT outsourcing, cloud auditor also must consider following points:

1) During cloud migration one or some parts of an application may not be compatible with cloud environment. Because the most of applications and related functions rely on internal corporate's network, not over the internet.

2) Web applications must be assessed to assure access controls, authentication, and monitoring.

3) Regardless any complexity, Identity and access management must be assessed, to ensure appropriate control access over resources.

4) Assessing endpoint systems ensure auditors that systems have sufficient security to gain legitimate access to cloud resources.

5) All communications and correspondence between vendors and corporate should be inspected based on SLA.

During the cloud auditing, audit models, standards and frameworks would be determined by audit team. As indicated in section four, cloud auditing can be performed as value-added or risk-based. The main differences between risk-based audit and value-added audit are that risk-based audit brings data security, data protection and risk assessment into focus however the concentration of value-added audit is on risk migration and cloud investment and their improvement [15,25 and 37]. Quality of services and risks assessment of cloud environment also are two important issues in firm by seeking an audit request through internal or external cloud auditors.

In a cloud computing environment, cloud computing audit can be conducted in an alternative way, in which the auditors intelligibly should comprehend the available technology of cloud computing thought a value-added method and the related value would be created once the organization adopts the approach. [25, 37]. And focusing on targeted attractive features to clients by the auditing work would provide followings available benefits, values and possibilities if cloud computing is adopted:

Solutions for every financial plan and necessity, more appropriate use of resources, raised flexibility, bigger agility and supported efficacy, ameliorated collaboration, cost avoidance, reformed cost model, access to novel technology, and developed security [25,29].

In general, the first step for a firm to adopt cloud computing is to select the right cloud vendor. Since cloud vendors have direct impact on cost, quality, and operational processes in cloud environments, thus, selection, and continuous evaluation of cloud vendor should be considered by cloud auditors. Auditing work in cloud computing requires

more effort than ordinary IT auditing processes, as it requires the support and supervision of wanted information technologies of an external vendor [12,15,16 and 19]. Important factors in vendor's selection and evaluation measurements are: financial heath, operational performance metrics, expertise, risk factors, etc.

The next crucial step is providing a service contract with strong service level agreements (SLAs). The best time for cloud auditing is before the contract is finalized and signed. In this step all contractual obligations should be clearly stated. Some of these obligations are: SLAs (Availability, Performance, support coverage), SLA security (Encryption, Data privacy, data retention, data destruction, security training and background check, control frameworks), compliance assessments (SSAE 16, ISEA 3402), penalties for non-performance, condition for terminating, subcontracting relationships (right of denial, access to subcontractor's ISAE 3402), etc.

Eventually, providing a comprehensive report is required. The report is written in a standard format and included all audited cloud sections. Preparing a complete report is a major factor by which the reputation of internal audit department is established such as: data storage, cost savings, security issues, cloud governance, risks and so on [39]. Cloud auditor's report contains five sections: objectives, procedures, findings, recommendations and limitations based on the policies, standards, risks and business process.

After the cloud auditing process, an organization gain comprehensive view of pros and cons of cloud environment in its business. Moreover, strengths, weaknesses, associated risks and security breaches are clearly realized. Logical solutions can be recommended by auditors and organization executives and board need to work out strategies for solving occurring IT-related imperfections and later emphasize their complete business process management [25].

VI. Frameworks and Standards

IT audit standards provide a set of criteria, guidance, frameworks, procedures and methodologies that help to determine the extent of audit steps in order to how an audit should be conducted and what audit reports should be issued for IT engagements.

The fast evolution of cloud computing services and lack of sufficient standardization for these services caused utilizing many traditional IT audit standards for cloud auditing. Security, privacy and SLA's are potential challenges and concerns by cloud computing. There are several active organizations which have a number of guidance, standards, frameworks and metrics to assess cloud computing environment such as: ENSIA (European Network and Information Security Agency), ISACA (Information Systems Audit and Control Association), CSA (Cloud Security Alliance), and NIST. The publications of these organizations can be robust references for cloud audits. In the following we explain some of these organizations in short:

A summary of the possible negative outcomes in information security was provided by ENISA to stakeholders. It is a completely consultative organization, at the same time, it has accredited research related to security issues, such as "Cloud Computing Risk Assessment" [24], published in 2009. This paper strongly recommended several key points such as: continuous trust between cloud vendors and clients, Data protection in large-scale environments, large-scale systems' interoperability, resiliency, and monitoring. ENISA is following up different cloud activities and has robust frameworks which can be utilized as a useful reference for cloud auditors such as: Managing security through SLAs, Critical cloud services, Cloud Security and Resilience Expert Group, Good practice guide for Governmental clouds, Incident reporting for Cloud Computing, Certification in the EU Cloud strategy, and Cloud Certification Schemes List (CCSL).

A non-commercial formation as CSA with the purpose of supporting the application of most suitable practices, aims to assure security in cloud environments. Access Management Guidance and Identity has been introduced by CSA [26], including the most optimal solutions to ensure secure access management and identities. CSA research areas include cloud standards, frameworks, certification, guidance and tools. Some of important CSA's published documents and frameworks which can be very useful for cloud auditors during auditing process are: Cloud Computing's Critical Areas of Focus and their Security Guidance, Top Threats to Cloud Computing [32], GRC (Governance, Risk and Compliance) Stack, Cloud Controls Matrix (CCM), Cloud-Trust Protocol, and Consensus Assessments Initiative Research.

ISACA is a leading global organization in the development, adoption, and practices for information systems [27,28]. The popular ISACA's framework for IT management and governance are Control Objectives for Information and Related Technology also known as COBIT [15, 19 and 38]. "Controls and Assurance in the Cloud" is one of ISACA publications consist of practical guidance to provide cloud governance and control frameworks through an audit program by using COBIT 5. "Cloud Computing Management Audit/Assurance Program" is another useful published resource providing guidelines for the finalization of a particular and especial assurance procedure by ISACA [12,27 and 28].

The Unite States Department of Commerce's non-regulatory delegation known as NIST, supports innovation through research, measurements, standards, business services and other programs [8, 26]. NIST has three Special Publication subseries: SP800, SP1800, and SP500. The NIST 800 series is a set of publications as result of exhaustive research work for optimizing the computer security and describe policies, procedures and guidelines [10,11,26]. These publications cover all NIST-recommended procedures and criteria for assessing, threats, vulnerabilities and risk mitigation. The publications can be utilized as directions for the implementation of safety norms and auditing procedures as juristic references [37].

VII. Conclusion

Cloud computing is the latest evolution in the IT outsourcing world. Cloud adoption brings benefit for enterprises such as: business agility, data availability, ease of use, cost savings, and sustainability, but these benefits must be weighed against potential risks. In this paper we have provided a comprehensive perspective in the field of cloud computing

audit. We discussed different approaches and techniques for auditing in Cloud environment that have strong benefit for cloud adopters and auditors. To contextualize and study Cloud auditing, we have investigated the implications of IT auditing, cloud computing and definitions for key concepts. We have then determined test steps, key controls, and additional factors which have to be considered in cloud environment. Finally, we have introduced active organizations and their appropriate standards and frameworks for cloud computing assessment and audit.

ACKNOWLEDGMENT

The present paper was supported by the University of Debrecen to development and research program for the project "Auditing and quality assurance strategies in Cloud Computing services". I am immensely honored and gratefully thank those whom I have had the pleasure to work with on this paper and other related manuscript and projects.

REFERENCES

[1] Kalaiprasath, R., R. Elankavi, and R. Udayakumar. "Cloud security and compliance-a semantic approach in end to end security." International Journal on Smart Sensing and Intelligent Systems 10 (2017): 482-495.

[2] David Balovich: "Sarbanes-Oxley Document Retention And Best Practices" by 3JM Company Inc., Lake Dallas, Tx, May 09, 2007, Creditworthy News.

[3] Al-Twaijry, A. A. M, Brierley, J. A, & Gwilliam, D. R. (2003). The development of internal audit in Saudi Arabia: An Institutional Theory perspective. Critical Perspective on Accounting, 14, 507-531. doi:10.1016/S1045-2354(02)00158-2.

[4] Savouk, O. (2007). Internal audit efficiency evaluation principles. Journal of Business Economics and Management, 8(4), 275–284.

[5] D.C. Chou, An investigation into IS outsourcing success: the role of quality and change management, Int. J. Inf. Syst. Chang. Manag. 2 (2) (2007) 190–204.

[6] Mousavi. SM.,et al.: "Increasing QoS in SaaS for low Internet speed connections in cloud", The 9th International Conference on Applied Informatics, Eger, Hungary Feb 1 2014, pp. 195-200.

[7] Yigitbasioglu, Ogan, Kim Mackenzie, and Rouhshi Low. "Cloud Computing: How does it differ from IT outsourcing and what are the implications for practice and research?." The International Journal of Digital Accounting Research 13 (2013): 99-121.

[8] P. P. Mell, T. Grance, "The NIST Definition of Cloud Computing", NIST Special Publication 800-145, National Institute of Standards and Technology Gaithersburg, MD 20899-8930, September 2011.

[9] YOUSEFF, L., BUTRICO, M. & DA SILVA, D. (2008): "Toward a Unified Ontology of Cloud Computing", Gce: 2008 Grid Computing Environments Workshop: 42-51.

[10] F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger, D. Leaf, NIST Cloud Computing Reference Architecture NIST Special Publication 500-292, 2011.

[11] Mousavi. SM., Fazekas.G.: "A Novel Algorithm for Load Balancing using HBA and ACO in Cloud Computing Environment", International Journal of Computer Science and Information Security, June 2016, 14(6), pp.48-52.

[12] S. Gadia, "Cloud computing: an auditor's perspective", ISACA (Information Systems Audit and Control Associatio) Volume 6, J. 6 (2009).

[13] Aceto, G., Botta, A., De Donato, W., & Pescapè, A. (2013). Cloud monitoring: A survey. Computer Networks, 57(9), 2093-2115.

[14] Mousavi. SM. et al: "A load balancing algorithm for resource allocation in cloud computing", Advances in Intelligent Systems and Computing, Recent Global Research and Education: Technological Challenges, Springer International Publishing 2017, vol 66(16), pp. 289-296.

[15] V. Raval, Risk landscape of cloud computing, ISACA J. 1 (2010).

[16] Mousavi. SM. et al: "Dynamic Resource Allocation in Cloud Computing", Journal Acta Polytechnica Hungarica, March 2017, 14(3), pp. 80-101.

[17] Gantz, Stephen D. The Basics of IT Audit: Purposes, Processes, and Practical Information. Elsevier, 2013.

[18] Belay, Z. (2007). A Study on effective implementation of internal audit function to promote good governance in the public sector. Presented to the "The Achievements, Challenges, and Prospects of the Civil Service Reform program implementation in Ethiopia" Conference Ethiopian Civil Service College Research, Publication & Consultancy Coordination Office.

[19] T.W. Singleton, IT audits of cloud and SaaS, ISACA J. 3 (2010) 1–3.

[20] De Smet, D, & Mention, A. (2011). Improving auditor effectiveness in assessing KYC/AMLpractices: Case study in a Luxembourgish context. Managerial Auditing Journal, 26(2), 182–203.

[21] J.A. Hall, Information Technology Auditing and Assurance, third edition South-Western Cengage Learning, Mason, OH, 2011.

[22] Mousavi. SM., Fazekas. G.: "Dynamic resource allocation using combinatorial methods in Cloud: A case study", 16th international conference CogInfoCom 2017, pp. 221-232.

[23] Yazdankhah, F, Honarvar, AR "An Intelligent Security Approach using Game Theory to Detect DoS Attacks in IoT." International Journal Of Advanced Computer Science And Applications 8.9 (2017): 313-318.

[24] Sookhak, M, et al. "Remote data auditing in cloud computing environments: a survey, taxonomy, and open issues." *ACM Computing Surveys (CSUR)* 47.4 (2015): 65.

[25] Chou, David C. "Cloud computing risk and audit issues." Computer Standards & Interfaces 42 (2015): 137-142.

[26] Mousavi. SM., Fazekas. G. (2017): "Dynamic resource allocation in Cloud Computing using a new hybrid Metaheuristic algorithm". PhD thesis 2017.

[27] Identity Management Audit/Assurance Program, ISACA, by ISACA,Identity Management, 2013.

[28] ISACA Issues Four New Audit Programs on Cloud Computing, Crisis Management, Security and Active Directory, ISACA, 2010.

[29] Mousavi. SM.,Fazekas. G.: "Increasing QoS in SaaS for low Internet speed connections in cloud", The 9th International Conference on Applied Informatics, Eger, Hungary Feb 1 2014, pp. 195-200.

[30] D.C. Chou, A.Y. Chou, Analyses of software quality and auditing, in: C.V. Brown, H. Topi (Eds.), IS Management Handbook, seventh editionCRC Press, Boca Raton, FL,2000.

[31] Internal Auditors, Global Institute of Internal Auditors (IIA), Available at http://www.theiia.org2012 (accessed November 1, 2012).

[32] Halpert, B. Auditing Cloud Computing: A Security and Privacy Guide, Wiley Corporate, 2011.

[33] Richard Bradford-Knox. "Approaches to and the Management of the Audit Process in the Food Industry", British Food Journal, 2017.

[34] Cloud Computing, European International Journal of Science and Technology (EIJST).

[35] NACM National Trade Credit Reports issued by trade credit report team, published on credit worthy and tradecreditreport[dot]com websites.

[36] Merhout. J.W., Havelka. D.,"Development of an Information Technology Audit Process Quality Framework". Conference: Reaching New Heights. 13th Americas Conference on Information Systems, AMCIS 2007.

[37] Kenneth G Crowther, Yacov Y. Haimes, M. Eric Johnson. "Principles for Better Information Security through More Accurate, Transparent Risk Scoring", Journal of Homeland Security and Emergency Management, 2010.

[38] David C. Chou. "Cloud computing: A value creation model", Computer Standards & Interfaces, 2015.

[39] Jaydip S., "Security and Privacy Issues in Cloud Computing", in book: Architectures and Protocols for Secure Information Technology Infrastructures, Edition: First Edition., Chapter: 1, Publisher: IGI-Global, USA, September, 2013.