Available online at www.alphanumericjournal.com

alphanumeric journal

The Journal of Operations Research, Statistics, Econometrics and Management Information Systems

Volume 2, Issue 1, 2014

2014.02.01.MIS.01

INFORMATION TECHNOLOGY AUDIT AND THE PRACTICE OF THE TURKISH COURT OF ACCOUNTS

Musa Kayrak*

Sayıştay Başdenetçisi, CISA, Sayıştay Başkanlığı, Ankara

Received: 03 March 2014
Accepted: 10 May 2014

Özet

Bilişim teknolojilerinin kamu ve özel sektörde yoğun kullanımı, fırsatlarla birlikte bilginin güvenliği, gizliliği, güvenilirliği ve bütünlüğü hususlarında birtakım güçlükleri de beraberinde getirmiştir. Aynı şekilde, iç kontrol ortamı ve denetim kanıtının doğasında ciddi değişikliklere yol açmıştır. Bu nedenle, denetimlerin başarılı bir şekilde yürütülebilmesi için yeni denetim prosedürlerinin oluşturulması zorunlu hale gelmiştir. Bu çalışma, genel hatlarıyla bilişim teknolojileri denetimini açıklamakta ve Türk Sayıştayının deneyimleri hakkında ayrıntılı bir izahat ve yüksek denetim örgütleri (YDK) için öneriler ortaya koymaktadır.

Anahtar Kelimeler: Bilişim Teknolojileri Denetimi, Türk Sayıştayı.

Jel Kodu: 038, H83,M42.

Abstract

Prevalent use of information technologies in both private and public sector has brought not only opportunities but also various challenges in terms of security, confidentiality, reliability and integrity of information. By the same token, it has led to a fundamental change in the internal control environment and nature of audit evidence. Hence, it has become compulsory to design new audit procedures in order for successful implementation of audits. This study broadly defines information technology audit and provides a comprehensive explanation of the experiences of the Turkish Court of Accounts and recommendations for supreme audit institutions (SAIs).

Keywords: Information Technology Audit, Turkish Court of Accounts.

Jel Code: 038, H83,M42.

*musakayrak@sayistay.gov.tr

1. Introduction

Drastic changes in information technologies altering nature of internal control environment and audit for the last 15 years have led to the information revolution which has imposed an inevitable transformation at each and every aspect of our lives. Not only everyday lives have been profoundly influenced by innovations introducing mobility, connectedness, easiness, and high quality (ITIF, 2007) but also nature of the business environments has been significantly reshaped by the new rules of the business in today's world which has already become a global village. Changes in the traditional decision-making process have fueled the greed for timely, relevant, value-added, coherent, and accurate information and in turn increased the dependency in information technologies. Likewise, public sector organizations have kept pace with digital revolution in order to meet the growing expectations for high quality, easiness, and transparency in public services (Kayrak, 2012a). As a consequence, digital revolution has created a new world described by four "I"s: Information, Intelligence, Integration, and Innovation (Hinnsen, 2012).

2. Information Technology Risks And Controls

In the early phase of the digital revolution First usage of information systems in financial departments was automating payrolls and recording them on the accounting books (Akbaş, 2011). Afterwards, introducing various information systems such as transaction processing systems, office support systems, management information systems, decision support systems and strategic information systems helps organizations manage information in its journey from data to knowledge and wisdom created at different levels of business (Topkaya, 2011). Today, intense use of information technologies in the business processes turns out to be an indispensable prerequisite of competitiveness to survive and grow in the challenging business environments.

Producing, processing, storing, achieving huge amount of data from every segments of the business requires newest and flexible technologies; however, this does not necessarily add value to organizations due to the fact that complicated technologies and plethora amount of information may lead to complexity, duplication, intolerability, and confusion. By the same token, it is equally noteworthy to figure out that use of information technologies gives rise to detrimental impacts of IT-related risks which should be mitigated within the framework of business risk management while keeping in mind that 100 percent security cannot be reached at any information technology environment.

Table 1: Risks with an IT origin (ECA, 2011)

Risk	IT-related risk source
Individual errors become systematic	Automation replacing manual operations
Failure to identify the performer	Electronic transactions not logged
Unauthorised access and changes to data	Electronic data not properly secured
Loss (destruction) of data	Electronic data not protected
Disclosure of clasified information	Electronic data not properly secured

Defining threats and vulnerabilities is key to launch a risk assessment and treatment and for this reason it would be naive to define any IT controls without an IT risk assessment. It is crucial to assess the IT risk assessment procedures and figure out impact of IT on financial statement assertions and the level of risk (Schroeder and Singleton, 2010).

In an organization where business processes financial or non-financial are carried out by the help of information systems and where information assets are threaten by the IT-related risks, traditional internal control objectives are closely integrated with IT controls. That is to say, control objectives in an information technology environment stay unchanged from those of a manual environment albeit the implementation may differ. For that reason, internal control objectives should be addressed IT-related business processes (ISACA, 2010).

IT controls may be categorized as preventive, detective and corrective controls as shown in the Table 2. Preventive controls help managements detect problems before they occur and prevent an error, omission or malicious act from occurring while detective controls detect and report the occurrence of an error, omission or malicious act. Corrective controls, on the other hand, are used to resolve problems and eventual errors discovered by detective controls and aimed at revising the system in a way to hinder the future occurrence of the same or similar problems (INTOSAI, 2007; ISACA, 2010; Kayrak, 2012a).

Table 2: IT controls

	Technical	**Administrative**	**Physical**
Preventive	Use of EncryptionSoftware, Intrusion Prevention Systems.	Employ Only Qualified Personnel, Segregate Duties	Locked Doors, Security Personnel.
Detective	Biometric Controls, Network Scanners	Audit Log Reviews, Compulsory Annual Leaves.	Physical Counting, Smoke Detector
Corrective	File Recovery from Backups	Insurance, Disaster Recovery Plan.	Hot-Warm-Cold Sites.

- Intense use of information systems in business processes has profoundly influenced the audit universe as well. It leads to alteration of the nature of audit evidence and trail; change the internal control environment; brings about suitable circumstances for fraudulent activities; and makes it compulsory to create new audit procedures (Ozkul, 2002; INTOSAI, 1996). In today’s audit profession, the role of IT audit becomes very fundamental to avoid financial fiascos like Enron and WorldCom (Senft and Galleos, 2009) or IT incidents that adversely affects the reliability and integrity of data audited.

3. Information Technology Audit

3.1. Information Technology Audit: Definition and Objectives

Information technology audit was often called electronic-data processing (EDP) audit due to main use of information technologies to manage data in the past. The terms “Information technology (IT) audit” and “information system (IS) audit” have been used in the recent decades because of increasing role of IT in the business environment which influenced change in the terminology.

IT audit can simply be explained as an audit of an organization’s IT systems, IT operations, IT governance and management and other related processes. According to the definition of Ron Weber, IT audit is “the process of collecting and evaluating evidence to determine whether a computer system (information system) safeguards assets, maintains data integrity, achieves organizational goals effectively and consumes resources efficiently” (Sayana, 2002 cited in Weber, 1988). Main goal of IT audit is to review and provide assurance about certain information criteria determined in accordance with the type, scope and objectives of the audit. The seven information criteria can be defined as follows (ISACA, 2007):

Effectiveness deals with information being relevant and pertinent to the business process as well as being delivered in a timely, correct, consistent and usable manner.

Efficiency concerns the provision of information through the optimal (most productive and economical) use of resources.

Confidentiality concerns the protection of sensitive information from unauthorized disclosure.

Integrity relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations.

Availability relates to information being available when required by the business process now and in the future. It also concerns the safeguarding of necessary resources and associated capabilities.

Compliance deals with complying with the laws, regulations and contractual arrangements to which the business process is subject, i.e., externally imposed business criteria as well as internal policies.

Reliability relates to the provision of appropriate information for management to operate the entity and exercise its fiduciary and governance responsibilities.

While the main goal of IT audit is data integrity and security in general, efficiency and effectiveness of using IT assets are also an important concern for the IT audit (Pathak, 2005). IT auditor may focus on the abovementioned information criteria as a whole or partly depending on the audit objectives. To illustrate, if the audit focus is to review IT governance in an auditee, efficiency and effectiveness would be the main information criteria. In the same way, integrity, availability and confidentiality are the main information criteria to give assurance if the audit focus is information security (Kayrak, 2012a).

When IT audit is carried out as a part of financial audit, the main audit focus will be reliability, integrity, confidentiality and availability of information owing to the fact that financial audits concentrate upon reliability of financial statements and legality and regularity of underlying transactions. An IT audit in the context of a financial audit aims at (ECA, 2011):

Understanding the overall impact of IT on key business processes;

Assessing management controls on IT processes;

Understanding how the use of IT for processing, storing and communicating information affects internal control systems, inherent risk and control risk;

Evaluating the effectiveness of controls on IT processes which affect the processing of information.

Furthermore, efficiency and effectiveness of information will be assessed in the case of performing an IT audit as a part of performance audit. A performance audit may have an IT focus when (ECA, 2011);

The audit focuses on the performance of IT systems;

The audit examines the efficiency and effectiveness of a business process and/or programme where IT is a critical tool for the organization delivering those services;

Data reliability is to be assessed.

3.2. IT Audit Methodology

While it is apparent that internal controls of the entities using complex IT systems mostly rely on IT controls, references to IT in international audit standards are rather marginal (Rechtman, 2009). Considering that international audit standards for SAIs (ISSAI) does not provide a comprehensive, up-to-date and exhaustive chapter for IT audit methodology, SAIs seem to implement different approaches toward developing IT audit methodologies. For instance, European Court of Auditors and National Audit Office of the United Kingdom preferred to launch a guideline for “financial audit in an IT environment” for the generalist auditors instead of preparing a purely technical IT audit guideline (ECA, 2011; NAO, 2002). However, the General Accountability Office of the USA prepared a separate IT audit guideline of “Federal Information System Controls Audit Manual” (GAO, 2009).

IT audit is carried out in accordance with the specific steps designed for planning, implementation and reporting of the audit work. While conducting an audit of IT systems, IT auditors are expected to comply with the following steps in accordance with a risk-based audit approach (Turkish Court of Accounts, 2013):

Determine the risks arising from the use of IT systems;

Identify the control mechanisms mitigating these risks;

Examine whether the required control mechanisms are established by the auditee, and if so, whether they are functioning effectively or not;

Assess internal control weaknesses;

Report the findings obtained in line with existing procedures.

IT auditors examine two types of controls in order to understand whether control mechanisms satisfactorily fulfill an expected level of maturity in accordance with needs of the business.

Firstly, general controls are related to structures, methods and procedures intended to ensure the continuity of the activities of all IT systems of the auditee. These controls create a reliable internal control environment for IT applications and application controls designed on those IT applications. That's why, they can be defined as controls relating to the environment within which IT applications are developed, maintained and operated (ISACA, 2010). General controls consist of the following areas:

Management controls

Physical and environmental controls

Network management and security controls

Logical access controls

Processing controls

System development and change management controls

Emergency and work continuity planning controls

Application controls, on the other hand, are designed at IT application level. They can be defined as "The policies, procedures and activities designed to provide reasonable assurance that objectives relevant to a given automated solution (application) are achieved" (ISACA, 2012). Pertaining to specific IT applications, application controls either manual (performed by users) or automated (performed by computer software) are procedures that are designed to ensure the integrity and confidentiality of data (ECA, 2011). They can be categorized as:

Input controls

Processing controls

Output controls

Data transmission controls.

IT audit methodology involves both compliance testing and substantive testing. While compliance testing is aimed at finding out whether IT controls are designed in line with management policies and procedure, substantive testing focuses on gathering evidences through testing auditee's data in relating to validity and propriety of transactions (Office of the Comptroller & Auditor General of India, 2006). IT auditors could follow either a system based approach or a direct substantive testing approach depending on the nature of audit. System based audit approach which includes both compliance and substantive testing concentrates on aspects of regularity, economy, efficiency and effectiveness besides evaluation of data integrity and data security. On the other hand, direct substantive testing approach requires selection and testing of a sample of transactions which will provide evidences to auditors in relating to validity and propriety of transactions (INTOSAI, 2002).

4. Experience of the Turkish Court of Accounts

4.1. Background Information

The experience of the Turkish Court of Accounts (TCA) relating to IT audit began more than a decade ago through applying data analysis techniques during compliance audits and IT audit of the Undersecretariat of Treasury in cooperation with an audit firm. On the other hand, first systematic and methodological approach to meet the rising needs for IT audit knowledge within the TCA and in the public sector could be accepted as the Twinning Project with the National Audit Office (NAO) of UK held between 2004 and 2007. Depending on the Twinning Project TCA drafted the first version of IT audit guideline, launched certain number of IT audits while improving data analysis knowledge (mainly ACL). As an extension of the twinning project, the TCA signed a protocol with the Scientific and Technological Research Council of Turkey (TUBITAK) to further develop its theoretical knowledge and experience in the field. Signed in 2007, the protocol mainly aimed at developing IT audit guideline, delivering information system security trainings to the IT auditors of the TCA and launching joint IT audits in public institutions. Within the scope of the protocol following outcomes were achieved:

- Review of the IT audit guideline of the TCA,
- A four month training program on subjects such as IT audit, certificate on Certified Information System Auditor (CISA), information security management system, network and operating system security, databases, business continuity, COBIT, and common criteria and
- Pilot IT audits.

The TCA organized an “IT Audit Self-Assessment (ITASA) Workshop” in collaboration with the “IT Working Group” of the European Organization of Supreme Audit Institutions (EUROSAI) in 2013 and prepared an action plan to determine the future of IT audit in the Court. Based on the methodological works, experiences through independent IT audits, and recommendations of the ITASA, the final version of the IT audit guideline of the Court was officially accepted and published by the Presidency of the TCA upon the approval of the Information Technology Steering Committee in 2013.

4.2. IT Audit Guideline

The IT audit guideline is aimed at guiding the auditors on how an IT audit is planned, performed and reported. INTOSAI guidelines and standards, Information Security Standards (ISO27K), ISACA guidelines (mainly COBIT 4.1 and Assurance Guideline) and the manuals of other countries and relevant entities are the main references of the guideline. Prepared with the assumption that it would be used by the auditors specialized on IT auditing (not generalist auditors), the guideline do not provide very much conceptual. Basic IT controls for the generalist auditors are provided in the Regularity Audit Manual of the TCA (TCA, 2013b).

The IT Audit Guideline of the TCA provides three main parts: Firstly, “Audit Planning” part explains the steps to be taken by IT auditors such as understanding the entity and its IT systems, identifying the systems having effect on financial statements, conducting system risk assessment, determining the audit strategy, and preparing the audit program. Secondly, “Assessing System Controls” is composed of control areas and provides a comprehensive framework in order to help IT auditors prepare audit programs and assess existence and effectiveness of controls in those areas. Finally, third part focuses on reporting and monitoring the audit results (TCA, 2013).

4.3. Main Findings of the IT Audit Practice of the TCA

The TCA has carried out independent IT audits, IT audits as a part of regularity audit and IT audits as a part of value for money audit. The most common and critical findings of the pilot IT audits in the last 10 years can be summarized as (Kayrak, 2012b):

- Lack of IT strategic management with IT strategic plans and IT steering committees established at an appropriate level;
- Lack of written and approved policies, plans, and guidelines;
- Weak IT risk management and value management;
- Issues regarding compliance with IT laws and regulations;
- Lack of formal IT project management;
- Inefficient IT organizations with lack of defined IT roles and responsibilities;
- Weak design of application controls on financial application;
- Poor physical and environmental conditions imposing important risks on business continuity;

- Lack of policies and monitoring in access management, password management and account management;

Lack of appropriate business continuity plans (BCP) and disaster recovery plans (DRP).

4.4. Use of IT in TCA Audits

Auditors of the TCA make use of information technology as much as possible so as to improve quality of the TCA audits including regularity audit, performance audit and IT audit. Main IT systems that TCA uniquely implements are the audit management system and the computer assisted audit software.

4.4.1. Audit Management System of the TCA: SAYCAP

SAYCAP, the audit management system tool of the TCA, is a customized software product developed between 2011 and 2012. The Presidency of the TCA made the final decision in favor of using this tailor-made AMS tool due to its high level of adaptability and flexibility which enables to meet all the requirements of the sui generis nature of the TCA audits. SAYCAP has already helped the TCA achieve following benefits (TCA, 2012):

- Improving efficiency and effectiveness of regularity audits;
- Carrying out timely audits;
- Measuring the planned costs of audits in order to improve programming and budgeting processes;
- Providing a high level of standardization among the works of all audit teams completely in line with regularity audit manual;
- Establishing a better quality control review system including hot and cold reviews;
- Producing timely management information to help senior management monitor audits and take necessary decisions;
- Facilitating information sharing in a systematic way among the auditors.

According to the statistics of the audit year 2013, the TCA has carried out the regularity audit of 489 auditees by the help of SAYCAP which has helped the auditors prepare 98243 electronic working papers and determine 964 inherent or control risks during understanding the auditee step of audits.

SAYCAP automates all the steps of regularity audit of the TCA and can be used to implement IT audits and performance audits as well. Furthermore, SAYCAP is based on an audit procedure approach which requires creating working papers for each and every single step of the audit. As a part of regularity audits, 37 audit procedures related to audit step of “understanding the IT systems of the auditee” are created and added to the audit procedure library and auditors are supposed to follow these procedures during regularity audits and may also add new one when necessary. These audit procedures relating to policy and strategy controls, software development and change management controls, logical access controls, physical controls and application controls (TCA, 2013b) are designed for generalist auditors and that’s why, auditors do not need to have in-depth IT audit knowledge and or IT skills to use them.

4.4.2. Computer Assisted Audit Software and System Design Project: SAYDAP

Currently, the TCA has an ongoing “Computer Assisted Audit Software and System Design Project” planned to be finalized at the end of 2013. The aim of the Project is to define the computer aided audit methodologies for the TCA and design and develop a flexible, modular and functional system which implements those methodologies. By the end of the Project following benefits will be fully achieved (TCA, 2013a);

- Regular data transfer from auditee in accordance with the regulation describing the methods, procedures and formats relating to the data gathering from the auditees;
- A portal for the auditees to upload their data;

- Automated data analysis on the off-line copies of auditee's data on a scheduled basis by the Application itself;
- Implementation of a vast variety data analysis techniques by the auditors;
- Carrying out basic data mining techniques such as nearest K neighbor, decision tree, forecasting and clustering analysis etc.

The first versions of the software have already been tested by the system analysts and a group of users and it is projected to use SAYDAP in the course of TCA audits of the year 2014.

5. Conclusion and Lessons Learnt

In today's world; rules, standards, expectations, values and risks are heavily affected by the information technologies. While people have easiness in getting accustomed to what Peter Hinnsen called this new phase digital revolution as "the new normal" (Hinnsen, 2012), public administrations including Supreme Audit Institutions do not act fast enough to achieve all the benefits of the IT transformation or get rid of the possible predicaments on their horizons. In today's world information is the biggest assets while change, flexibility, speed and innovative thinking are sidekicks of it. However, SAIs do not operate in isolated environment free from requisites of the new normal; in other words, they also need to adjust themselves to challenges of the information revolution both in terms of administrative processes and also auditing activities in the public sector.

According to Gartner, in 2012 total amount of IT investments are 3,6 trillion Dollar around the world (Gartner, 2012) and the pace of increase in IT investments will not likely to decrease in the near future. On the other side of the coin, data breaches, system failures and inefficient use of IT turn out to be common IT-related issues regardless of the development level of countries. This not only reveals insufficient IT management and governance practices but also give glints of where the future of audit goes. In parallel to this, researches point out that some auditors show continued interest in leveraging technology-enabled auditing as their top priorities for improvement (Protiviti, 2013).

Based on the experiences and lessons learnt of the TCA on IT audit, the following actions can be suggested to flourish IT auditing within the framework of supreme audit functions:

1. Is IT audit "the elephant in the room"?: Traditional approaches to the audit are no longer efficient enough to satisfactorily fulfill the roles and responsibilities of SAIs; hence, it crucially important not to overlook, ignore or leave unaddressed the growing needs for IT audit.

2. Make a fresh start - self-assessments: "IT Self-Assessment" and "IT Audit Self-Assessment" are the best ways to figure out the current situation of IT audit in SAIs and draw a clear roadmap for the future in harmony with one's own needs.

3. Need for IT auditor- start from scratch: Identifying generalist auditors who are capable and who are interested in becoming IT auditors is the best way to begin.

4. Establishing an appropriate level of IT organization: Best practices among SAIs show that either creating separate IT audit unit or distributing IT auditors in audit groups are main options.

5. Actions speak louder than words - time to start IT audits: Pilot audits in collaboration with some IT experts, audit firms or other public institutions would be preferred in the transition period.

6. Need for IT audit methodology: It is essential to have an IT audit guideline for SAIs but it is equally vital to implement a methodology in line with internationally accepted standards. ITAF™: A Professional Practices Framework for IS Audit/ Assurance, 2nd Edition; COBIT Assurance Guideline; COBIT 3, 4.1 and 5; ISO/IEC 27K; ISO/ IEC 15408 and ISO/IEC 38500; NIST SP 800, ITIL; TOGAF; PMBOK and PRINCE2 are some of the existing international frameworks which IT auditor can make use of in preparing IT audit guidelines and IT audit programs.

7. Improving awareness of stakeholders: SAIs could be key actors to highlight IT risks in the public sector and raise the awareness of people and Parliaments. This can be achieved through the IT audits of most critical IT systems of the country so that findings of IT audits would be appealing to a large number of stakeholders.

8. Continuing professional education and training: Lack of expertise on IT audit is a common issue among SAIs with some exceptional cases such as the SAIs of Norway, Switzerland and UK. According to international standards, IT auditors are expected to maintain professional competence through appropriate continuing professional education and training (ISACA, 2013). This requires better training planning in SAIs to improve IT awareness, IT knowledge and skills in IT auditing.

9. Getting certified: Being Certified Information System Auditor (CISA) is the best to receive recognition from auditees, auditors, and other stakeholders. To do so, SAIs need to motivate and support IT auditors with necessary training activities and financial aids as well.

10. International cooperation and collaboration: International cooperation among SAIs in the form of symposiums, seminars, trainings and workshops is the best way to follow up the developments in the field of IT auditing and implement them in SAIs' policies and procedures.

..

References

1. Ahmet Topkaya, (2011) "Management of Information Technologies and Audit Principles", Journal of External Audit: July, August, September 2011, No. 5, pp. 23-36.
2. Anantha S. Sayana, (2002) "The IS Audit Process", ISACA Journal: 2002, No.1 http://www.isaca.org/Journal/Past-Issues/2002/Volume-1/Pages/The-IS-Audit-Process.aspx (Accessed at 09.05.2014).
3. Dan Schroeder and Tommie Singleton, (2010) "Implementing the IT-Related Aspects of Risk-Based Auditing Standards" , The CPA Journal: July 2010, pp. 66-71.
4. Davut Ozkul, (2002) IS Audit, Unpublished Master Thesis, Ankara.
5. European Court of Auditors –ECA, (2011) "Guideline for Audit of IT Environment", Luxembourg: ECA.
6. Gartner, (2012) "Gartner Says Worldwide IT Spending On Pace to Surpass $3.6 Trillion in 2012", http://www.gartner.com/it/page.jsp?id=2074815, (Accessed at 27.11.2013).
7. General Accountability Office – GAO, (2009) "Federal Information System Controls Audit Manual", USA: GAO, http://www.gao.gov/new.items/d09232g.pdf, (Accessed at 10.05.2014).
8. Gürkan Akbaş, (2011) "Important of Basic IT Audit within a Financial Audit", Journal of External Audit: July, August, September 2011, No. 5, pp. 9-16.
9. Information Technology and Innovation Foundation - ITIF, (2008), "Why Is the Digital Information Revolution So Powerful?" http://www.itif.org/files/DQOL-1.pdf (Accessed at 01.12.2013).
10. International Organization of Supreme Audit Institutions - INTOSAI, (1996) "IT Controls Student Notes", Vienna:INTOSAI.
11. International Organization of Supreme Audit Institutions – INTOSAI, (2002) "Information Technology Audit General Principles", Vienna: INTOSAI http://intosaiitaudit.org/India_GeneralPrinciples.pdf (Accessed at 01.12.2013).
12. International Organization of Supreme Audit Institutions – INTOSAI, (2007) "Introduction to IT Audit", Vienna INTOSAI.
13. ISACA, (2007) COBIT 4.1, USA:ISACA.
14. ISACA, (2010) CISA Review Manual 2010, USA:ISACA.
15. ISACA, (2012) "ISACA Glossary of Terms", USA:ISACA.
16. ISACA, (2013) "A Professional Practices Framework for IS Audit/Assurance", USA: ISACA.
17. Jagdish Pathak, (2005) Information Technology Auditing, Germany: Springer.
18. Musa Kayrak, (2012a) "Information Technology Audit in the Context of Information Criteria", Journal of Turkish Court of Accounts: October-December 2011, No. 87, pp. 143-167.
19. Musa Kayrak, (2012b) "IT Audit Training Notes to the Assistant Auditors of the TCA", Ankara: TCA.
20. National Audit Office – NAO, (2002) "Auditing in an IT Environment", UK: NAO.
21. Office of the Comptroller & Auditor General of India, (2006) "Manual of Information Technology Audit- Volume I", http://saiindia.gov.in/english/home/Our_Process/Audit_Methology/Manuals/ITAM%20Vol_I.pdf (Accessed at 09.05.2014).
22. Peter Hinnsen, (2012) The New Normal, Belgium: MachMedia.
23. Provitivi, (2013) "Hot Topics in Public Company Transformation", http://www.protiviti.com/en-US/Documents/White-Papers/Risk-Solutions/PCT-IPO-Readiness-Key-Market-Research-Trends-Protiviti.pdf (Accessed at 30.11.2013).
24. Sandra Senft and Frederick Galleos, (2009) Information Technology and Control (Third Edition), NewYork: CRC Press.
25. Turkish Court of Accounts, - TCA, (2012) SAYCAP User Manual, Ankara:TCA.

26. Turkish Court of Accounts, - TCA, (2013a) Answers to IT as Enabler Questionnaire, EUROSAI ISSAP Working Group, Ankara.: TCA.
27. Turkish Court of Accounts - TCA, (2013b). "Regularity Audit Manual", Ankara: TCA.
28. Yigal Rechtman, (2009) "Evaluating Software Risk as Part of a Financial Audit", The CPA Journal: June 2009, pp.68-71.