IT AUDIT – INTRODUCTION OF THE IT AUDIT IN AN ORGANIZATION*

Elda HOXHAJ**

Muhasebe Bilim
Dünyası Dergisi
Mart 2018; 20(1); 90-115

ABSTRACT

Business performance, value and success are more and more depending on information technology governance and on the related IT risk management efficiency. To completely accomplish the main objectives of Auditing, internally or externally sourced, in this era, the introduction of an additional professional tool, the IT Audit, is being increasingly considered as an absolute and indispensable need. This paper aims to treat and emphasize, through comparison and analysis, the necessity and relevance of IT Audit, in both public and private enterprises. IT Audit, as a new important field and strong risk assessment tool of Auditing, drives to a higher level of efficiency and ensures that the enterprise system is getting the maximum business value / performance for itself and for all stakeholders too. Highlighting the evidenced advantages of an effective IT Audit through best practices, the paper's purpose is to strongly motivate and encourage other organization as well to introduce the IT Audit in their org chart.

Keywords: Information Technology Audit, IT Efficiency, Information Systems Performance, Certification Of IT Audit

JEL Classification: M42, O32-3

BT DENETİMİ - BİR ÖRGÜTTEKİ BİLGİ TEKNOLOJİLERİ DENETİMİNE GİRİŞ

ÖZ

İş performansı, değeri ve başarısı, bilgi teknolojisi yönetişimine ve ilgili bilgi teknolojileri risk yönetim verimliliğine bağlı olarak gittikçe artmaktadır. Denetimin ana hedeflerini gerçekleştirme amacıyla (dahili veya harici kaynaklardan olsa da), Bilgi Teknolojileri denetiminin ek bir profesyonel araç olması giderek mutlak ve vazgeçilmez bir ihtiyaç olarak kabul edilmektedir. Bu makale, karşılaştırma ve analiz yoluyla bilgi teknolojileri denetiminin hem kamu hem özel işletmelerdeki gerekliliğini, önemini ele almayı ve vurgulamayı amaçlamaktadır. Denetimin yeni önemli bir alanı ve

---

* This paper was presented at 14th International Conference on Accounting, hold by MODAV in TIRANA/ ALBANIA, on October 11-13, 2017 and prepared in accordance with criticism. Date of submission: 21.11.2017; Date of acceptance: 05.02.2018.

** PhD Candidate at the Department of Accounting, Faculty of Economy, University of Tirana; orcid.org/0000-0003-0293-9663, elda_hm@yahoo.com

güçlü risk değerlendirme aracı olan bilgi teknolojileri denetimi, daha yüksek bir verimlilik seviyesine yönlendirir ve kurumsal sistemin kendisi ve tüm paydaşları için de azami işletme değerini / performansını elde etmesini sağlar. Bu makalenin amacı; bir taraftan etkili bilgi teknolojileri denetiminin kanıtlanmış avantajlarını en iyi şekilde uygulamalarla vurgulamak, diğer taraftan ise, diğer kuruluşları da teşvik etmek ve bilgi teknolojileri denetimini kendi kuruluş şemasında sunmaktır.

Anahtar Kelimeler: Bilgi Teknolojisi Denetimi, Bilgi Teknolojisi Verimliliği, Bilgi Sistemleri Performansı, Bilgi Teknolojileri Denetimi Sertifikası

JEL Sınıflandırması: M42, O32-3

1. INTRODUCTION

1.1. The Definition of Auditing and its Main Fields

The term "*audit*" has been derived from the Latin word "*audire*" which means to hear (www.dictionary.com).

The Institute of Chartered Accountants of India (ICAI[1]) defines that "An audit is the independent examination of financial information of any entity, whether profit oriented or not, and irrespective of its size or legal form, when such an examination is conducted with a view to expressing an opinion thereon" (ICAI Nature, Objective and Scope of Audit)[2].

The IIA[3] (The Institute of Internal Auditors) definition (https://na.theiia.org/standards-guidance/mandatory-guidance/Pages/Definition-of-Internal-Auditing.aspx) of Internal Auditing states the fundamental purpose, nature, and scope of internal auditing: "Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes".

[1] The Institute of Chartered Accountants of India (ICAI) is a statutory body established by an Act of India Parliament for regulating the profession of Chartered Accountancy in the country. Refer also to www.icai.org.
[2] See more info to https://resource.cdn.icai.org/46524bosinter-p6-cp1.pdf
[3] IIA is a trustworthy, global, guidance-setting body, which provides internal audit professionals worldwide with authoritative guidance organized in the IPPF as mandatory guidance and recommended guidance. www.theiia.org

INTOSAI[4] with its ISSAI (International Standards of Supreme Audit Institutions), IFAC[5] (International Federation of Accountants) through its IAASB[6], the IIA, AICPA[7] (The American Institute of Certified Public Accountants) with its FASB (Financial Accounting Standards Board) and other international and national standard–setting bodies, although in different ways, define three basis of audit.

The ISSAI framework contains three fundamental auditing principals, which determines and provides the most comprehensive definition of three fundamental basis of audit (INTOSAI ISSAI 100):

- Financial audit – focuses on determining whether an entity's financial information is presented in accordance with the applicable financial reporting and regulatory framework. This is accomplished by obtaining sufficient and appropriate audit evidence to enable the auditor to express an opinion as to whether the financial information is free from material misstatement due to fraud or error.
- Performance audit – focuses on whether interventions, program and institutions are performing in accordance with the principles of economy, efficiency and effectiveness and whether there is room for improvement. The aim is to answer key audit questions and to provide recommendations for improvement.
- Compliance audit – focuses on whether a particular subject matter (ex. activities, financial transactions and information) is in compliance with authorities identified as criteria (ex. rules, laws and regulations, budgetary resolutions, policy, established codes, etc.).

[4] The International Organization of Supreme Audit Institutions (INTOSAI) operates as an umbrella organization for the external government audit community. For more than 50 years it has provided an institutionalized framework for supreme audit institutions to promote development and transfer of knowledge, improve government auditing worldwide and enhance professional capacities, standing and influence of member SAIs in their respective countries (http://www.intosai.org/about-us.html)

[5] IFAC is the global organization for the accountancy profession dedicated to serving the public interest by strengthening the profession and contributing to the developments of strong international economies (http://www.ifac.org/about-ifac)

[6] The International Auditing and Assurance Standards Board is an independent standard-setting body that serves the public interest by setting high-quality international standards for auditing, assurance, and other related areas, and by facilitating their adoption and implementation (http://www.iaasb.org/about-iaasb)

[7] AICPA is the world's largest member association representing the accounting profession in the United States (http://www.aicpa.org/About/Pages/default.aspx)

1.2. Auditing Objectives - Risk Assessment, One of Core Objectives of Auditing

The fundamental objective of all national[8] or international[9] assurance and auditing standard-setting bodies, by setting high-quality national or international standards in regard, is to serve to the public interest, enhancing the quality and uniformity of practice throughout the world and strengthening public confidence in the global auditing and assurance profession[10].

The purpose of an audit is to enhance the degree of confidence of intended users in the financial statements. This is achieved by the expression of an opinion by the auditor on whether the financial statements are prepared, in all material respects, in accordance with an applicable financial reporting framework. In the case of most general-purpose frameworks, that opinion is on whether the financial statements are presented fairly, in all material respects, or give a true and fair view in accordance with the framework. An audit conducted in accordance with ISAs and relevant ethical requirements enables the auditor to form that opinion. (IAASB Handbook 2016-17 ISA 200 p 80).

In conducting an audit of financial statements, the overall objectives of the auditor are (IAASB Handbook 2016-17 ISA 200 p 82):

a) To obtain reasonable assurance about whether the financial statements as a whole are free from material misstatement, whether due to fraud or error, thereby enabling the auditor to express an opinion on whether the financial statements are prepared, in all material respects, in accordance with an applicable financial reporting framework; and

b) To report on the financial statements, and communicate as required by the ISAs, in accordance with the auditor's findings.

As stated in the last IAASB Handbook (IAASB Handbook 2017 ISA 200 p 81), the ISAs contain objectives, requirements and application and other explanatory material that are designed to support the auditor in obtaining reasonable assurance.

---

[8] National auditing standard setters are from: Australia, Brazil, Canada, China, France, Germany, Hong Kong, India, Japan, Mexico, New Zealand, South Africa, The Netherlands, United Kingdom and United States of America as well as the Nordic Federation.

[9] See also (http://www.iaasb.org/about-iaasb)

[10] The International Auditing and Assurance Standards Board is an independent standard-setting body that serves the public interest by setting high-quality international standards for auditing, assurance, and other related areas, and by facilitating their adoption and implementation (http://www.iaasb.org/about-iaasb)

The ISAs require that the auditor exercise professional judgment and maintain professional skepticism throughout the planning and performance of the audit and, among other things:

- Identify and assess risks of material misstatement, whether due to fraud or error, based on an understanding of the entity and its environment, including the entity's internal control.
- Obtain sufficient appropriate audit evidence about whether material misstatements exist, through designing and implementing appropriate responses to the assessed risks.
- Form an opinion on the financial statements based on conclusions drawn from the audit evidence obtained.

AAS 2, issued by ICAI, states that the objective of an audit of financial statement is to enable an auditor to express an opinion on such financial statements. A financial audit has:

- A basic objective of examining whether the accounts are true and fair.
- An incidental objective of detecting errors and frauds.

OECD (SIGMA Paper No. 19 1998) claims that Audit may be carried out to satisfy the requirements of management (internal audit), or by the supreme audit institution (SAI), or any other independent auditor, to meet statutory obligations (external audit). A particular task of internal audit is to monitor management control systems, report to senior management on weaknesses and recommend improvements.

2. IT RISK AS A COMPONENT OF THE OVERALL RISK UNIVERSE OF THE ORGANIZATION, INTRODUCING IT AUDIT AND ITS ROLE IN IT GOVERNANCE

2.1. Defining IT

At the very beginning, the most complicated IT item was a simple calculator machine. From that time on, the world has witnessed significant progress and evolution in regard to information technology. Technology embeds quite everything each people encounter now. Organizations worldwide are allocating more and more resources to continuously develop IT projects.

IT has different meaning to different organization. Even inside the same industry can happen that two organizations may have fundamentally different IT environments. Unfortunately, IT has not a clear and universal definition.

2.2 IT As A Risk Area And its Mitigation

Organizations invest large amounts of capital to implement a new information system, market research and enter new markets, develop and lunch new products, conquer new business contracts, create and manage national or international partnerships and face the dynamic perspective and the increasing global economic challenges with continuous improvement and timely response.

These investments are made with the aim to bring about positive change to the organization, but at the other side they also present a relevant degree of risk.

Consequently, the result of success or not can be critical to the strategy of an organization, as well as have a significant impact on the organization's reputation and business efficiency.

In the era, when technology plays a critical role in the life of an organization, many projects and investments are focused around information technology. IT related investments tend to come like fashion, and all the organizations worldwide respond to it.

Practically, IT related implementation projects are very complex initiatives that require the involvement of more than IT staff and have a significant impact in the entire business project.

How to think about IT within an organization?

"*A chain is only as strong as its weakest link*" (UK Proverb)

Consequently…"An organization is only as strong as its weakest person / process."

IT matters become more complex as going further deeper within a single organization. Information technology projects and environments, throughout an organization, involve various processes and procedures, in-house or outsource people that are fraught with challenges that must be carefully considered to ensure success for the organization itself.

Every organization is exposed to a huge unacceptable risk that can result from issues related IT as: projects scope and objectives are poorly defined; insufficient user participation and

contribution; lack of expertise and competent human resources support; inappropriate or wrong technology choices; lack of sufficient knowledge about modifying, alternating or changing technologies.

Global Technology Audit Guide 12 (IIA GTAG 12 2009), within its context, emphasis the significant impact failed or challenged projects has in an organization and provides some examples of possible risk that include:

- Disruption of service to customers.
- Loss of competitive advantage.
- Fines from failed regulatory compliance.
- Loss of revenue.
- Negative impact on reputation.
- Delays in deploying critical strategic initiatives, products, or processes.
- Loss of expected return-on-investment.
- Loss of critical business and IT personnel.
- Facility closure or damage.
- Loss of shareholders/investors.

2.3 IT Governance Risks – Aligning the Organization and IT

The risks an organization faces include strategic risk, environmental risk, market risk, credit risk, operational risk and compliance risk. In many organizations IT risk is considered to be a component of operational risk (ISACA Risk IT Framework 2009).

The Basel II Committee defines operational risk as: "The risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external

events"[11] (BIS Operational Risk Supporting Document to the New Basel Capital Accord, 2007, http://www.bis.org/publ/bcbsca07.pdf).

As quite all the risk categories imply risks components related IT, it better not to frame or depict IT risk with a hierarchic dependency. IT is a key that enables and facilitates the business initiatives, which related risks go along with the strategic risk of the organization. The same applies for credit risk; where unsecure IT can lead to lower credit ratings.

The business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise. It consists of IT-related events and conditions that could potentially impact the business. IT risk is not purely a technical issue; IT risk is business risk (ISACA Risk IT Framework 2009).

The Risk IT Framework, provided by ISACA, dedicated to helping enterprises manage IT-related risk, considers IT risk is a component of the overall risk universe of the enterprise, as shown in the below figure (BIS Operational Risk, Supporting Document to the New Basel Capital Accord, http://www.bis.org/publ/bcbsca07.pdf) .

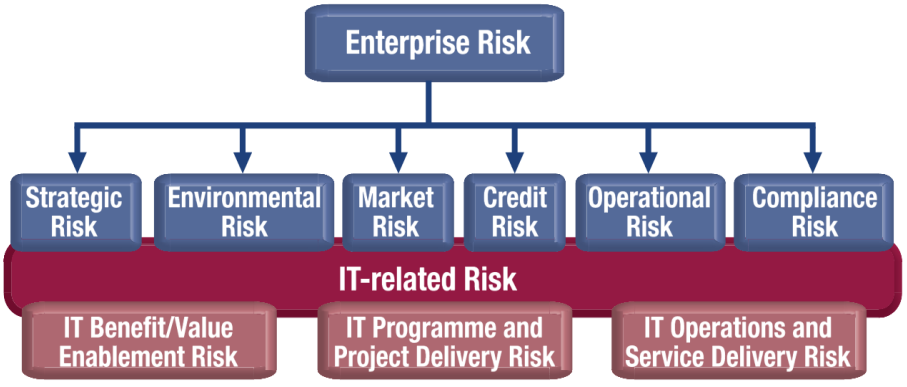

Figure 1: IT Risk in the Risk Hierarchy

Source: ISACA Risk IT Framework 2009

[11] Supporting Document to the New Basel Capital Accord, Operational Risk, pg. 2 http://www.bis.org/publ/bcbsca07.pdf

2.4 History of IT Audit

Electronic Data Process (EDP) Auditing has been the first step of the IT Auditing and developed largely motivated from the rise in technology in accounting systems, the need of IT control and the impact of the computers on the ability to perform attestation services (https//en.wikipedia.org).

Comparing to auditing as a whole, IT auditing has a short history and remains a constantly changing and developing field.

The introduction of computer technology into accounting system changed the way financial data was stored, retrieved and controlled. Up to 1960s, the auditing profession was still out of computer. The implementation of various computerized accounting system brought the need for auditor to become familiar with EDP concepts in the business environment.

Auditing & EDP book (www.aicpa.org), released by AICPA in 1968, was the first guide which provided for auditors instruction on how EDP audits could be documented and offered examples on how internal control reviews could be processed.

Auditing controls in the computer systems were becoming increasingly critical to the operations of their organizations. ISACA [12] got its start in 1967 and formalized in 1969 (previously named EDP Auditors Association) as a need for a centralized source of information and guidance in the field.

In 1977 was published the first edition of *Control Objectives*. Now days this publication is known as Control Objectives for Information and related Technology (CobiT) (www.isaca.org).

Major Failure Events

Equity Funding Corporation of America is the first case known of misuse of information technology (’64-’73). The discovered fraud and the process of confirmation that the insurance policies were fake, brought for the first time the auditors to perform an audit through the computer. The IT failure case of **AT&T** had a huge worldwide impact that effected commerce and communication. This event awoke the need for assurance in the IT services. **Enron** and

[12] Today, ISACA’s constituency—more than 140,000 strong worldwide—is characterized by its diversity. Constituents live and work in more than 180 countries and cover a variety of professional IT-related positions—to name just a few, IS auditor, consultant, educator, IS security professional, regulator, chief information officer and internal auditor (http://www.isaca.org/About-ISACA/History/Pages/default.aspx)

Arthur Andersen LLP scandal remains the largest bankruptcy in U.S. history, with its business strategy of "peak and decline the stock price" (https//en.wikipedia.org).

As reported on August 2005 (CIO Magazine Holmes 2005*)*, a large U.S. government agency had to scrap a US $170 million virtual case file management system development project due to schedule delays, cost overruns, and technical difficulties.

These events and other similar failure events worldwide have heightened the need for more accurate, reliable and secure systems and the focus to improve the control and the standards, especially these involved IT.

2.5 Assessing the Risk – Moving to a Risk-Based Approach

More and more organizations are moving to a risk-based audit approach.

The IIA states that the Mission of Internal Audit[13] articulates what internal audit aspires to accomplish within an organization. Its place in the New International Professional Practices Framework (IIA IPPF 2017) is deliberate, demonstrating how practitioners should leverage the entire framework to facilitate their ability to achieve the Mission and to enhance and protect organizational value by providing risk-based and objective assurance, advice, and insight.

IT presents risk factors that are unique to accounting, auditing and systems. IT itself brings risk to the organization regarding the different types of system, business processes and financial accounting processing. That risk would not exist if IT would not being present (Singleton ISACA Journal 2014).

The risk management process model, according the Risk IT framework groups key activities into a number of processes, grouped into three domains: Risk Governance, Risk Evaluation and Risk Response (ISACA Risk IT Framework 2009).

[13] See full info at https://na.theiia.org/standards-guidance/Pages/Mission-of-Internal-Audit.aspx

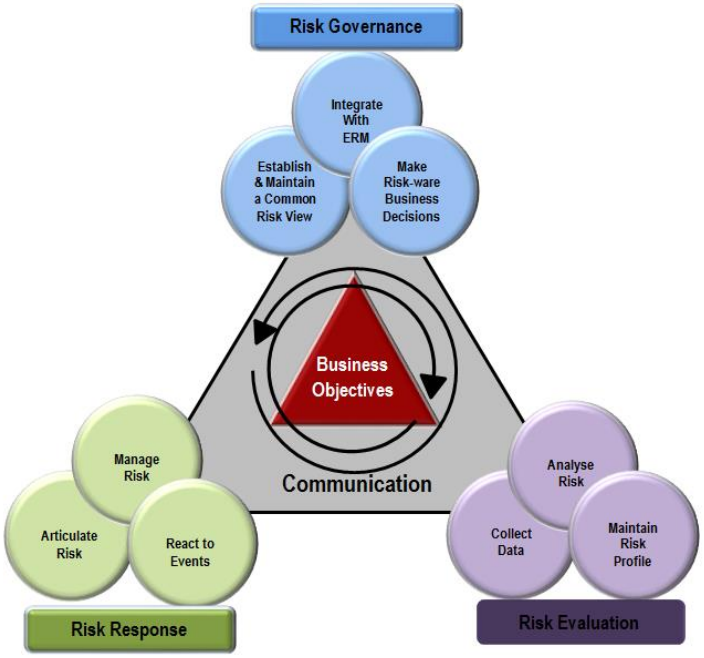

Figure 2. Risk IT Framewok, ISACA 2009

Identifying IT usage is one the very first challenges one IT Audit faces when determining the involvement of IT audit resources.

In order to properly determine how allocate IT audit resources, a lot of issues connected to information technology need to be correctly addressed.

Most of the companies do not conduct a separate IT Risk assessment. The responsibility related IT risk assessment generally falls to the IT Audit.

The Risk IT framework process model provides a detailed analysis of the roles carrying responsibility and/or partial accountability for the process of Accountability for IT Risk Management. Management guidelines include goals and metrics at different levels and Responsible, Accountable, Consulted and Informed (ISACA Risk IT Framework RACI charts 2009).

All the individual (RACI) charts regarding the business processes across the three Risk IT domains are integrated in the below table:

Table 1. Consolidated RACI Chart

	Roles	BOARD	CEO	CRO	CIO	CFO	Enterprise Risk Committee	Business Management	Business Process Owner	Risk Control Functions	HR	Compliance and Audit
	Key Activities											
RISK GOVERNANCE	**RG1 - Establish and mamintain a common risk view**											
	RG1.1 Perform enterprise IT risk assessment	I	A	R	R	C	I	R	C	R	C	C
	RG1.2 Propose IT risk tolerance thresholds	I	I	C	R	C	I	A	C	C		C
	RG1.3 Approve IT risk tolerance	A	C	C	C	C	R	C	C	C	C	C
	RG1.4 Align IT risk policy	C	A	R	R	R	C	R	R	R	R	C
	RG1.5 Promote IT risk-aware culture	A	R	R	R	R	R	R	R	R	R	R
	RG1.6 Encourage effective communication of IT risk	R	R	R	R	R	R	A	R	R	R	R
	RG2 - Integrate with ERM											
	RG2.1 Establish and maintain accountability for IT risk management	A	R	R	R	R	I	I	I	C	C	C
	RG2.2 Co-ordinate IT risk strategy and business risk strategy	A	R	C	R	C	C	R	C	C	C	I
	RG2.3 Adapt IT risk practices to enterprise risk practices.			C	A/R	C	I	C	C	R	C	C
	RG2.4 Provide adequate resources for IT risk management	A	R	C	R		I	C	R	C	C	
	RG2.5 Provide independent assurance over IT risk management	A/R	C	C	C	C	C	C	C	C	C	C
	RG3 - Make risk-aware business decisions											
	RG3.1 Gain management buy-in for the IT risk analysis approach		C	A/R	R	C	C	C	C	R	C	C
	RG3.2 Approve IT risk analysis		I	R	C	C	A	I	R	I	I	I
	RG3.3 Embed IT risk considerations in strategic business decision making	I	C	C	A/R	C	C	C	C	R	C	I
	RG3.4 Accept IT risk	I	I	C	R	C	R	A	R	C		I
	RG3.5 Prioritise IT risk response activities		I	A	R	I	C	C	R	R		I
RISK EVALUATION	**RE1 - Collect data**											
	RE1.1 Establish and maintain a model for data collection	I	I	A/R	C	C	C	C	C	C		C
	RE1.2 Collect data on the operating environment		I	A/R	C	I	I	C	I	I	I	C
	RE1.3 Collect data on risk events		I	A	R	C	I		C	C		I
	RE1.4 Identify risk factors			A	R	I	I	C	C	R	C	C
	RE2 - Analyse risk											
	RE2.1 Define IT risk analysis scope		I	R	C	I	C	A	R	C		C
	RE2.2 Estimate IT risk		I	R	C	C	I	A/R	R	R		C
	RE2.3 Identify risk response options			C	C	C	R	A	R	R		I
	RE2.4 Perform a peer review of IT risk analysis			A/R				I		I		I
	RE3 - Maintain risk profile											
	RE3.1 Map IT resources to business processes			I	R			C	A/R	C		I
	RE3.2 Determine business criticality of IT resouces		C		R		C	A	R			I
	RE3.3 Understand IT capabilities			C	A/R				C	C		I
	RE3.4 Update IT risk scenario componenets			C	R	I	C	C	A	R		C
	RE3.5 Maintain the IT risk register and IT risk map		I	A	R	I	I	I	R/C	C		I
	RE3.6 Develop IT risk indicators			A	C			C	C	R	C	C
RISK RESPONSE	**RR1 - Articulate risk**											
	RR1.1 Communicate IT risk analysis results.		I	R	C	C	C	A	R	R	C	I
	RR1.2 Report IT risk management activities and state of compliance.	I	I	C	R	I	A	I	I	I	I	C
	RR1.3 Interpret independent IT assessment findings	I	I	A/R	R	I	I	I		C	I	C
	RR1.4 Identify IT-related opportunities		I	I	R	I	I	A	R	R	I	I
	RR2 - Manage risk											
	RR2.1 Inventory controls		I	A/R	C	I	I	C	C	R		C
	RR2.2 Monitor operational alignment with risk tolerance thresholds			C	C		I	A	R	R		C
	RR2.3 Respond to discovered risk exposure and opportunity	I	A	C	R	C	I	R	C	C	C	
	RR2.4 Implement controls	I	A	C	R	C	I	R	C	C	C	I
	RR2.5 Report IT risk action plan progress	I	I	I	R	I	I	I	A	R	I	I
	RR3 - React to event											
	RR3.1 Maintain incident response plans	I	I	I	R	C	I	I	A	R	C	I
	RR3.2 Monitor IT risk			C	I	I	I	I	A	R	C	R
	RR3.3 Initiate incident response	I	I	I	I	I	I	R	A	R	C	I
	RR3.4 Communicate lessons learned from risk events	I	I	A/R	R	C	I	C	C	R	C	I

Source: ISACA, Risk IT Framework (Source of Detailed Data Collected)

As emphasis in the integrated table, the role of Audit is responsible for 3 key activities: Promote IT Risk-aware culture, Encourage effective communication of IT risk and Monitor IT risk.

Audit is consulted and informed for the major parts of key activities of the three domains.

2.6 Management of IT Auditing - IT Audit Work

GTAG 11, *Developing the IT Audit plan* (IIA GTAG 11 2008) states that management of many organizational factors are considered when developing the audit plan, such as the organization's industry sector, revenue size, type, complexity of business processes, and geographic locations of operations.

Two factors having a direct impact on the risk assessment and in determining what is audited within the IT environment are its components and role. For example:

- What technologies are used to perform daily business functions?
- Is the IT environment relatively simple or complex?
- Is the IT environment centralized or decentralized?
- To what degree are business applications customized?
- Are some or all IT maintenance activities outsourced?
- To what degree does the IT environment change every year?

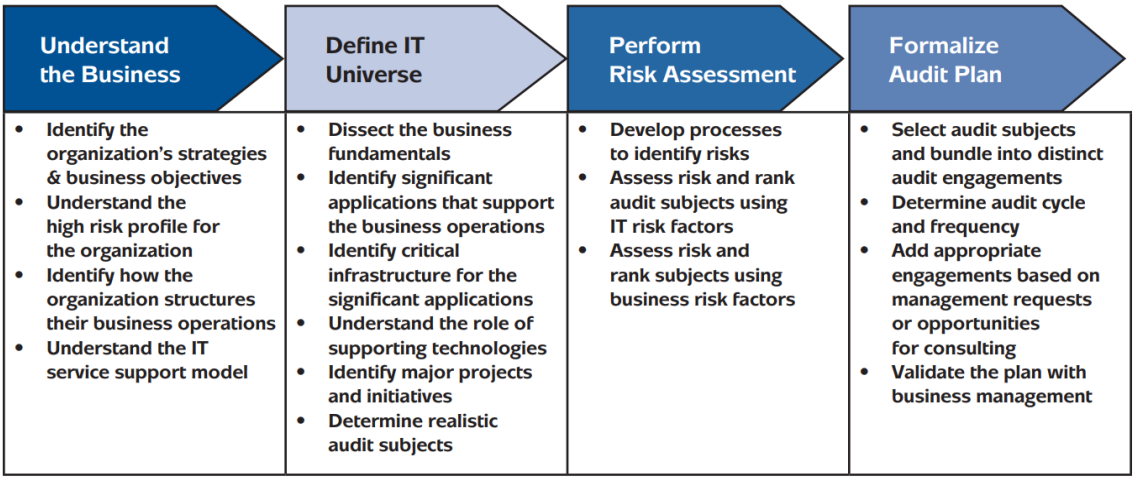

Figure 3. The IT Audit Plan Process (IIA GTAG 11)

2.7 IT Auditing -A Continuing Process

Auditing could not be understood as a single isolated issue, enhancing the degree of confidence means continuity. Auditing is a continuing assurance process of control, assessment and monitoring.

The internal audit activity must assist the organization in maintaining effective controls by evaluating their effectiveness and efficiency and by promoting continuous improvement. The internal audit activity must evaluate the adequacy and effectiveness of controls in responding to risks within the organization's governance, operations, and information systems regarding the (IIA Standard 2130 A1):

- Achievement of the organization's strategic objectives.
- Reliability and integrity of financial and operational information.
- Effectiveness and efficiency of operations and programs.
- Safeguarding of assets.
- Compliance with laws, regulations, policies, procedures, and contracts.

GTAG 3, *Continuous Auditing* (IIA GTAG 3) - identifies what must be done to make effective use of technology in support of continuous auditing and highlights areas that require further attention.

Continuous monitoring encompasses the processes that management puts in place to ensure that the policies, procedures, and business processes are operating effectively.

The audit activity's approach to, and amount of, continuous auditing depends on the extent to which management has implemented continuous monitoring. A continuous audit approach allows internal auditors to fully understand critical control points, rules, and exceptions.

Audit assurance is a statement regarding the adequacy and effectiveness of controls and the integrity of information. (IIA GTAG 3 2005)

Figure 4. Continuous Assurance (IIA GTAG 3 -Continuous Auditing)

3 PROFESSIONAL REQUIREMENTS FOR IT AUDITOR, CERTICATION OF IT AUDIT

IES 8 - *Professional Competence for Engagements Partners Responsible for Audits of Financial Statements* (IAESB IES 8)[14] provides a table of 8 technical competences areas and respective learning outcomes. Two of these competences areas, which require an "intermediate" level of proficiency, clearly encounter IT: Governance and risk management; Information technology.

ISACA audit programs have been developed and reviewed by leading audit and assurance professionals worldwide. ISACA (Journal volume 3 2010) outlines eight categories of business knowledge that IT audit and assurance professionals need to understand:

1. How is the enterprise *organized*?
2. How is the enterprise *governed*?
3. Under what *laws/regulations* does the enterprise operate?
4. What are the enterprise's *business processes*?
5. How does the enterprise *operate*?
6. How does the enterprise use *technology*?

[14] See more details on IES 8 professional requirements on http://www.ifac.org/system/ files/publications/ files/2017-Handbook-of-International-Education-Pronouncements.PDF

7. How does the enterprise *finance* itself?
8. How does the enterprise *measure business success*?

3.1. Certifications of It Audit

Organizations are engaging greater focus on their core internal capabilities to create the in-house IT Auditors. The lack of internal capacities, the increasing complexity of IT Audit, cost reductions and optimization of IT governance and control are some of the issues that lead an organization to the need of an outsourced IT Auditor.

Organizations place more weight in real-world experience and performance-based certifications (ISACA Loeb News Release 2017).

CISA – Certified Information Systems Auditor is the key ISACA qualification for IT Auditors and a global standard for information systems audit, control and security professionals.

CIA – Certified Internal Auditor, issued by IIA, covers four main areas of auditing, one of which Information Technology related.

ISMS (Information Security Management System) is a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process (certified by ISO/IEC 27001)[15].

Public accounting firms and practitioners, who obtain a **WebTrust business** license from the AICPA and CICA (Canadian Institute of Chartered Accountants), can provide assurance services to evaluate and test whether a particular ecommerce service meets the selected Trust Services principles and criteria (www.webtrust.org).

4 GLOBAL STANDARDS, COMPLIANCE, FRAMEWORK, GUIDELINES THAT LEAD TO BEST PRACTICES

The rapid progressed technology environment could render useless quite the most of the IT control baselines internally developed by an organization, in a short period of time.

[15] More info about ISMS can be found on https://www.iso.org/isoiec-27001-information-security.html

An organization itself could not be able to develop individual baseline that generate deliverables for all applications and technologies.

4.1. Global Standards

The particular nature of IT Audit and the specific required skills to perform such audits require standards that apply specifically to IT Auditing.

-**ISA 330**, *The Auditor's Responses to Assessed Risks*, (IAASB ISA 330 2006) deals with auditor's responsibility to design and implement responses to the risks in accordance with ISA 315. (IAASB ISA 315 - Identifying and Assessing the Risk of Material Misstatements through Understanding the Entity and Its Environments).

-**ISAE 3402**, *Assurance Reports on Controls at a Service Organization* was the first global assurance standard for reporting on controls at a service organization, exposure draft issued in December 2009 by the IAASB (IAASB ISAE 3402 2011).

-**SSAE 16**, *Reporting on Controls at a Service Organization*, was issued by AICPA in April 2010. SSAE 16 effectively replaced SAS 70 as the standard for reporting on service organizations.

-**ISO 27001**– The International Organization for Standardization (ISO) published this internationally recognized generic information security standard, which began as a British Standard (BS7799), and evolved into an ISO standard known as ISO 27001.

-**Information System Audit and Assurance Standard 1008** Criteria, issued by ISACA, defines mandatory requirements for IS auditing and reporting (ISACA IS Audit and Assurance Standard 1008 Criteria 2013).

-**IIA standard 2110**, *Governance*, states*: "*the internal audit must assess whether the information technology governance of an organization supports the organization's strategies objectives".

4.2. Regulatory Compliance

Different laws and regulations around the world are mandating the use of internal controls and risk management practices and the privacy of personally identifiable information, including the Sarbanes-Oxley Act and Basel II Accord.

4.3. Frameworks

One of the main challenges in creating and executing IT audit work is to be able to start with a set of IT control objectives and select an appropriate framework (composed of phases, activities, and tasks).

- IAASB **"Framework on Audit Quality"** (IAASB Framework on Audit Quality 2014) gives a relevant attention to one of contextual factor, which is "Information Systems". The nature and the quality of an information system may potentially affect the audit quality and the overall financial reporting quality.
- The **Information Technology Assurance Framework (ITAF)– A professional Practices Framework for IS Audit / Assurance,** issued by ISACA **(**ISACA ITAF 2014)[16], is a comprehensive and good-practice-setting reference model that: establish standards that addresses IS audit, defines terms and concepts related to IS assurance and provides guidance related IS audit.
- **The Abu Dhabi IT Architecture & Standards Framework** – covers all aspects of an IT environment and includes: Business, Access & Presentation, Applications, Data, Integration, Infrastructure, Security and Operations.
- **COSO [17] ERM [18]** - the Framework defines essential enterprise risk management components, discusses key ERM principles and concepts, suggests a common ERM language, and provides clear direction and guidance for enterprise risk management.

4.4. Global Guidelines

- The Institute of Internal Auditors (www.theiia.org) has published **17 Global Technology Audit Guides**, which address timely issues related information technology (IT) management, control and security.

[16] For additional information regarding ITAF refer to http://www.isaca.org/Knowledge-Center/Research/Documents/ITAF-3rd-Edition_fmk_Eng_1014.pdf

[17] The Committee of Sponsoring Organizations of the Treadway Commission (COSO) is a joint initiative of the five private sector organizations (AICPA, IIA, AAA, IMA FEI) and is dedicated to providing thought leadership through the development of frameworks and guidance on enterprise risk management, internal control and fraud deterrence. https://www.coso.org/Pages/default.aspx

[18] Additional information regarding Enterprise Risk Management could be fount at https://www.coso.org/Pages/erm.aspx

- **The ITAF guidelines,** issued by ISACA (ISACA ITAF 2014), supporting the standards, divided in three categories; General Guidelines (2000 series); Performance guidelines (2200 series) and Reporting guidelines (2400 series).
- ITAF tools and techniques guidance provides guidance for IS audit and assurance professionals through **COBIT 5** family of products.

5 IT AUDIT BEST PRACTICES – A GLOBAL REVIEW

In the report of IT Policy Compliance Group, that covers benchmarked practices within information security within IT audit function across more than 3'000 organizations, COBIT resulted the best primary practice guidance (Guidance for Best Practices in Information Security and the IT Audit, IT Policy Compliance Group 2009).

COBIT is an IT governance framework and supporting tool set that allows managers to bridge the gaps amongst control requirements, technical issues and business risk.

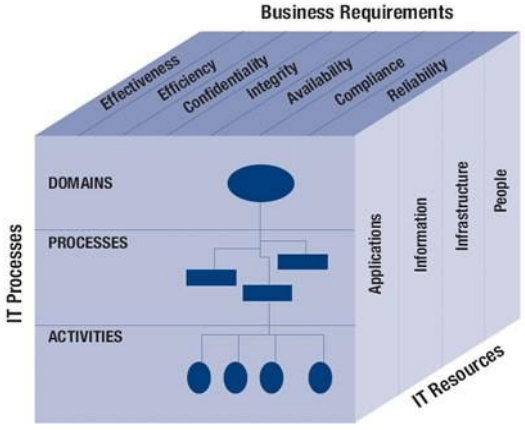

Figure 5. COBIT Structure, ISACA

According to the information provided by ISACA, COBIT has a worldwide use[19].

In Turkey: COBIT use is mandated by the Banking Regulator, Banking Regulation and Supervision Agency (BRSA) and for all Banks in the country. The Turkish Court of Audit, the country's Supreme Audit Institution, for performance of its IT Audits, uses COBIT.

[19] See more details at http://www.isaca.org/COBIT/Documents/Recognition-table.pdf

European Court of Audit uses COBIT in the performance of its Audits, including IT Governance reviews.

Albanian SAI uses COBIT. In 2015 was published the Albanian version of COBIT 4.1 (www.klsh.org).

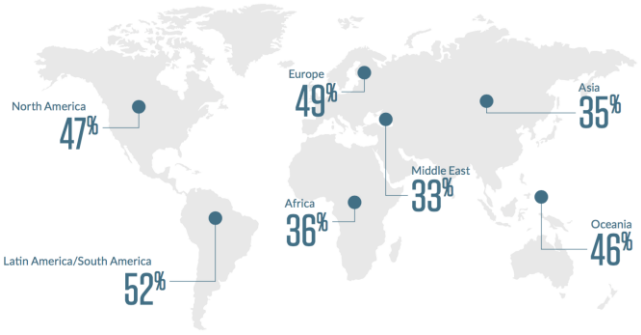

Figure 6. "Yes" Response of Having An IT Audit In The Organization (**source**: ISACA & Protiviti[20], A Global Look at IT Audit Best Practices 2016)

Table 2. Within organization, IT Audit reports to…

	Africa	Asia	Europe	Latin America/ South America	Middle East	North America	Oceania
CAE	47%	41%	51%	75%	91%	64%	63%
A director under the CAE	8%	8%	6%	12%	0%	10%	6%
CEO	28%	23%	26%	13%	9%	13%	19%
CIO	3%	10%	8%	0%	0%	2%	0%
Reports through some other function	14%	18%	9%	0%	0%	11%	12%

Source: ISACA & Protiviti, A Global Look at IT Audit Best Practices 2016

5.1 IT Auditing – An Adaptive Process In Albania

Albanian SAI (KLSH) is the first institution in Albania that has adopted the guidance toward IT Audit (started from 2015, KLSH is the best practice in this field):

[20] Protiviti is a global consulting firm which consulting solutions span critical business problems in technology, business process, analytics, risk, compliance, transactions and internal audit. For more info about the company refer to www.protiviti.com.

- *The Information Technology Control Objectives* (COBIT) book was made available in Albanian language in July 2015, being the first step of efforts to implement IT Audit in the Albanian SAI.
- *IT Audit Manual* was published on Aug. 2015, product of EUROSAI Information Technology Working Groups (WGITA) and the INTOSAI Development Initiative (IDI) for defining the rules and standards of Information Technology Audit.

6 IT Audits performed from KLSH in the last 3 years (www.klsh.org).

The Albanian Ministry of Finance published in May 2010 its first Internal Audit Manual. One the required audit field was the IT Audit, especially for the high risk capital projects and Information Technology. In this manual, IT Audit is considered components of a new field in Auditing, which is based on systems.

The law no. 114 (Oct. 2015) *"On Internal Auditing in the Public Sector"* was approved by the Albanian Parliament and applied to all units in the public sector (government units, state funds organizations and other financed by public funds). The law includes IT Audit as one of the main fields of auditing (alongside to financial, performance and compliance audit fields) and is mandatory for

The Board of the Albanian Financial Supervisory Authority (AMF Regulation no 38 2015), in May 2015, had deliberated a special regulation on the *minimum of the object and the contents of the audit report* required for to financial institutions under its authority. The audit report should contain "assessment of the quality and adequacy of the information technology system" (Art. 3, 1/d)

The Bank of Albania decision no. 42 / 2011, "*For the Registered Auditors of Banks…*" in the explanatory annex regarding the risk assessments require to the auditors to describe the IS/IT organization and administration assessing the adequacy, reliability and compliance to the bank activity. Assessment of the level of used technology, is as well required (www.bankofalbania.org).

6 MAIN FINDINGS AND CONCLUSIONS

Regardless of the organization or the industry, IT is critical to maintaining a competitive advantage, managing enterprise risks, achieving business objectives and challenging future projects.

Lack of the appropriate, careful and continuous attention on each individual IT challenge may result in undesirable financial and operational outcomes, wasted resources and time, loss of reputation and trust.

Understanding the relevant risks to the organization and understanding how technology affects and mitigates these risks, is one of the critical duties of IT Audit.

IT audit comes in help to the organizations, individuals find security while using Internet, and the same time helps commerce and communication to effectively develop and progress.

Increased ability to mitigate risks, reductions in the cost of assessing internal controls, increased confidence in financial results, improvements to financial operations and reductions in financial errors and the potential for fraud are some of the expected benefits that might result of implementing IT Auditing (IIA GTAG 11).

IT audit plays a critical role in auditing the core systems in order to support the financial audit.

IT auditing takes that one step further and evaluates the controls around the information with respect to confidentiality, integrity, and availability. While a financial audit will attest to the validity and reliability of information, the IT audit will attest to the confidentiality of the information, the integrity of the information and in situations where availability is a key factor will also attest to the availability and the ability to recover in the event of an incident. One of the key factors in IT auditing and one that audit management struggles with constantly, is to ensure that adequate IT audit resources are available to perform the IT audits (INFOSEC Institute 2017).

To accomplish the IT audit, IT depended organizations can find, motivate and develop internal professional capacities to create an internal IT auditor. If such specific professional internal capacities are missing, outsources certified IT Auditor could be engaged.

IT AUDIT remains a constantly changing and developing field.

More and more organizations, global frameworks, standards and regulations are moving to a risk-based audit approach.

All the detailed considerations in the recent IAASB handbooks (IAASB The Handbook Vol 3 2016-2017), related information system, shows that IAASB and IFAC are highly deliberating the importance of information system and its critical impact in the audit quality, a forward clear vision which may potentially lead to establishment of additional future ISA related IT / IS.

IES 8 (IAESB 2016) offers a sound base and become a potential subject to develop new ISA addressed to IT Audit.

Most of the regulations worldwide that mandate the use of Internal Control do not address IT controls directly. Implying the need for an adequately controlled IT environment, these regulatory areas remain potential subjects in the IT audit universe.

REFERENCES

Abu Dhabi Digital Government. 2013. The Abu Dhabi IT Architecture & Standards (IT A&S), https://www.abudhabi.ae/pdfdirectview/en/299582/blaetterkatalog/blaetterkatalog/pdf/complete.pdf, (Access Date: 10.10.2017)

Albanian Financial Supervisory Authority (AMF), the Board. 2015. Regulation no. 38, Art. 3, 1/d,http://www.amf.gov.al/pdf/ligje/208_Rregullore%20nr.%2038%2028.05.2015.pdf, (Access Date: 10.10.2017)

American Institute of Certified Public Accountants (AICPA). 2010. Statement on Standards for Attestation Engagements (SSAE) No. 16 - Reporting on Controls at a Service Organization.

American Institute of Certified Public Accountants/Canadian Institute of Chartered Accountants.2010.WebTrust Program for Certification Authorities, http://www.webtrust.org/homepage-documents/item65306.pdf,(Access Date: 09.10.2017)

American Institute of Certified Public Accountants. 1968. Auditing & EDP, Davis, G. (New York 1968)

American Institute of Certified Public Accountants. 2012. White Paper, Evolution of Auditing: Fromthe Traditional Approach to the Future Audit,https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/whitepaper_evolution-of-auditing.pdf,(Access Date: 25.09.2017)

American Institute of Certified Public Accountants, About AICPA, http://www.aicpa.org/About/Pages/default.aspx,(Access Date: 25.09.2017)

Bank for International Settlements (BIS). 2007. Supporting Document to the New Basel Capital Accord, Operational Risk, pg. 2, http://www.bis.org/publ/bcbsca07.pdf, (Access Date: 09.10.2017)

Bank of Albania.2011. Regulation no. 42 For the Registered Auditors of Banks…, https://www.bankofalbania.org/web/Rregullore_Per_ekspertin_kontabel_te_autorizuar_te_bankave_dhe_degeve_te_bankave_te_huaja_1294_1.php?kc=0,28,0,0,0, (AccessDate: 09.10.2017)

Committee of Sponsoring Organizations of the Treadway Commission (COSO), issued on 2004, last update 2017, Enterprise Risk Management, https://www.coso.org/Pages/erm-integratedframework.aspx, (Access Date: 17.09.2017)

History of Information Technology Auditing,https://en.wikipedia.org/wiki/History_of_information_technology_auditing, (Access Date: 10.10.2017)

Holmes, A. 2005. "Why the G Men Aren't IT Men", CIO Magazine Online, Aug. 15, 2005, https://www.cio.com/article/2437801/it-organization/why-the-g-men-aren-t-i-t--men.html, (Access Date: 30.09.2017)

IAASB. 2006. International Standard on Auditing (ISA) 330 - The Auditor's Responses to Assessed Risks, https://www.ifac.org/system/files /publications/files/Basis_for_Conclusions Clarity-1.pdf , (Access Date: 02.09.2017)

IAASB. 2009. International Standard on Assurance Engagement (ISAE) 3402 - Assurance Reports on Controls at a Service Organization,

IAASB. 2014. Framework on Audit Quality, P. 33 Ref. 5.4, par. 95-100, https://www.ifac.org/system/files/publications/files/A-Framework-for-Audit-Quality-Key-Elements-that-Create-an-Environment-for-Audit-Quality-2.pdf

Information Security Management System,https://www.iso.org/isoiec-27001-information-security.html, (Access Date: 07.10.2017)

INFOSEC Institute. 2017. http://resources.infosecinstitute.com/it-audit-introduction/#gref, (Access Date: 02.09.2017)

Institute of Chartered Accountants of India (ICAI), Nature Objective and Scope of Audit, Chapter 1, P. 2https://resource.cdn.icai.org/46524bosinter-p6-cp1.pdf, (Access Date: 16.09.2017)

Institute of Internal Auditors (IIA). 1941. Standards and Guidance, Mandatory Guidance, Definition of Internal Auditing, https://global.theiia.org/standards-guidance/mandatory-guidance/Pages/Definition-of-Internal-Auditing.aspx, (Access Date: 16.09.2017)

Institute of Internal Auditors. 2008. Global Technology Audit Guide 11 - Developing the IT Audit plan, https://chapters.theiia.org/montreal/ChapterDocuments/GTAG%2011%20-%20Developing%20the%20IT%20Audit%20Plan.pdf, (Access Date: 16.09.2017)

Institute of Internal Auditors. 2008. Global Technology Audit Guide 3 - Continuous Auditing

Institute of Internal Auditors. 2008. Global Technology Audit Guide 12 - Developing the IT

Audit Plan

Institute of Internal Auditors. 2009. Global Technology Audit Guide 12 - Auditing IT Projects, P. 3

Institute of Internal Auditors. 2017. Certification - CIA, https://global.theiia.org/certification/cia-certification/Pages/CIA-Certification.aspx, (Access Date: 10.10.2017)

Institute of Internal Auditors. 2017. International Standards for Professional Practice of Internal Auditing (IPPF-Standards), https://na.theiia.org/standards-guidance/Public%20Documents/IPPF-Standards-2017.pdf , (Access Date: 16.09.2017)

Institute of Internal Auditors, Mission of Internal Audit, https://na.theiia.org/standards-guidance/Pages/Mission-of-Internal-Audit.aspx, (Access Date: 16.09.2017)

International Auditing and Assurance Standards Board, About IAASB, http://www.iaasb.org/about-iaasb, (Access Date: 06.10.2017)

International Federation of Accountants, About IFAC, http://www.ifac.org/about-ifac, (Access Date: 01.10.2017)

International Federation of Accountants, International Accounting Education Standards Board. 2017. Handbook of International Educations Pronouncements, IES 8, P.100, http://www.ifac.org/system/files/publications/files/2017-Handbook-of-International-Education-Pronouncements.PDF, (Access Date: 06.10.2017)

International Federation of Accountants, International Auditing and Assurance Standards Board. 2016-2017. Handbook, Volume 1, International Standard on Auditing (ISA) 200 – Overall Objectives of the Independent Auditor and the Conduct of an Audit in Accordance with International Standards on Auditing, P. 80-82, http://www.ifac.org/system/files/publications/files/2016-2017- IAASB-Handbook-Volume-1.pdf, (Access Date: 06.10.2017)

International Organization for Standardization. 2017. ISO/IEC 27000 Family – Information Security Management System (ISMS),https://www.iso.org/isoiec-27001-information-security.html (Access Date: 09.10.2017)

International Organization of Supreme Audit Institutions (INTOSAI), About-Us, http://www.intosai.org/about-us.html, (Access Date: 28.05.2017)

International Organization of Supreme Audit Institutions. 2013. ISSAI 100 – Fundamental Principles of Public-Sector Auditing, P. 5, http://www.issai.org/en_us/site-issai/issai-framework/3-fundamental-auditing-priciples.htm, (Access Date: 01.10.2017)

ISACA&Protiviti.2016. A Global Look at IT Audit Best Practices, https://www.protiviti.com/sites/default/files/united_states/insights/6th-annual-it-audit-benchmarking-survey-isaca-protiviti-2017.pdf, (Access Date: 03.09.2017)

ISACA. 2009. Risk IT Framework, RACI charts, P.37

ISACA. 2009. Risk IT Framework, http://www.isaca.org/Knowledge-Center/Research/Documents/Risk-IT-Framework_fmk_Eng_0610.pdf?regnum=391273, (AccessDate: 25.09.2017)

ISACA. 2010. Journal volume 3, Business Skills for the IT Audit and Assurance Professional, https://www.isaca.org/Journal/archives/2010/Volume-3/Pages/Business-Skills-for-the-IT-Audit-and-Assurance-Professional.aspx?utm_referrer, (Access Date: 10.10.2017)

ISACA. 2013. Information System Audit and Assurance Standard 1008 Criteria, https://www.isaca.org/Knowledge-Center/Standards/Documents/1008-Criteria.pdf, (Access Date: 28.05.2017)

ISACA. 2013. Journal Volume 2, How to Properly Audit, https://www.isaca.org/Journal/archives/2013/Volume-2/Documents/13v2-How-to-Properly-Audit.pdf, (Access Date: 18.11.2017)

ISACA. 2014. COBIT Global Regulatory and Legislative Recognition, http://www.isaca.org/COBIT/ Pages/Recognition.aspx, (Access Date: 25.09.2017)

ISACA. 2017. Certification – CISA, http://www.isaca.org/Certification/CISA-Certified-Information-Systems-Auditor/Pages/default.aspx, (Access Date: 10.10.2017)

ISACA. 2017. Press Room, News Release, Loeb M. (ISACA CEO), http://www.isaca.org/About-ISACA/Press-room/News-Releases/2017/Pages/Survey-Cyber-Security-Skills-Gap-Leaves-1-in-4-Organizations-Exposed-for-Six-Months-or-Longer.aspx, (AccessDate: 19.11.2017)

IT Policy Compliance Group. 2009. Guidance for Best Practices in Information Security and the ITAudit,http://eval.symantec.com/mktginfo/enterprise/other_resources/b-guidancefor best_practices_in_information_security_and_it_audit-september_2009_OR_2875202.en-us.pdf,(Access Date: 03.09.2017)

KLSH (Albanian SAI). 2015. IT Audit Manual, http://www.klsh.org.al/ web/it_ audit_ manual_ 1904.pdf, (Access Date: 10.09.2017)

KLSH (Albanian SAI). 2015. The Information Technology Control Objectives (COBIT), http://www.klsh.org.al/web/cobit_1983.pdf; (Access Date: 10.09.2017)

http://www.klsh.org.al/web/COBIT_4_1_Objektivat_e_Kontrollit_te_Teknologjise_se_Informacionit_2859_1.php, (Access Date: 10.09.2017)

Kuvendi i Republikes se Shqiperise (Albanian Parliament), Oct. 2015. The law no. 114 "On Internal Auditing in the Public Sector", http://www.qbz.gov.al/botime/ fletore_zyrtare/2015/PDF-2015/195-2015.pdf, (Access Date: 10.09.2017)

Republika e Shqiperise (Republic of Albania), Ministria e Financave (Ministry of Finance). 2016. Manuali i Auditimit te Brendshem (Internal Audit Manual), http://aku.gov.al/wp-content/uploads/2016/06/REPUBLIKA-E-SHQIPERISE-MINISTRIA-E-FINANCAVE.pdf , (Access Date: 10.09.2017)

The Organization for Economic Co-operation and Development (OECD). 1998. SIGMA Paper No. 19, Effects of European Union Accession, Part 1: Budgeting and Financial Control, Appendix 3, https://stats.oecd.org/glossary/detail.asp?ID=4762, (Access Date: 21.11.2017)