

Using TELOS for the planning of the information system audit

D P Drljaca¹ and B Latinovic²

¹Europrojekt centar Banja Luka, Republic of Srpska, Bosnia and Herzegovina

²Pan European University Banja Luka, Faculty of Information Technologies, Republic of Srpska, Bosnia and Herzegovina

E-mail: drljacad@gmail.com

Abstract. This paper intent is to analyse different aspects of information system audit and to synthesise them into the feasibility study report in order to facilitate decision making and planning of information system audit process. The TELOS methodology provides a comprehensive and holistic review for making feasibility study in general. This paper examines the use of TELOS in the identification of possible factors that may influence the decision on implementing information system audit. The research question relates to TELOS provision of sufficient information to decision makers to plan an information system audit. It was found that the TELOS methodology can be successfully applied in the process of approving and planning of information system audit. The five aspects of the feasibility study, if performed objectively, can provide sufficient information to decision makers to commission an information system audit, and also contribute better planning of the audit. Using TELOS methodology can assure evidence-based and cost-effective decision-making process and facilitate planning of the audit. The paper proposes an original approach, not examined until now. It is usual to use TELOS for different purposes and when there is a need for conveying of the feasibility study, but not in the planning of the information system audit. This gives originality to the paper and opens further research questions about evaluation of the feasibility study and possible research on comparative and complementary methodologies.

1. Introduction

The auditing of the information systems in the public administration institutions is a serious business process that requires good planning and project-oriented approach. This is important since the auditing process commits funds, resources such as personnel and time that should be managed properly in order to maximise auditing process effect, minimise occupancy of the resources and to provide as best as possible auditing material for obtaining of auditors opinion.

Feasibility study aims to objectively and rationally discover and define strengths and weaknesses of an existing business or proposed a project, as well as the opportunities and threats present in the environment, the resources needed for the implementation and chances for success [1].

It helps in the decision-making process and as such has to evaluate and predict all the possible strengths and weaknesses of the system while in the contemplative (thinking) phase, to enable savings and to prevent losses occurred without full implementation. The study provides an overview of the number of the audit aspects.

At the present, the auditing of information systems in the public administration institutions in most of the countries is voluntarily or in the frame of the internal audit process. Some institutions, such as



the banks, are legally obliged to perform the audit of information system primarily to ensure security and safety of the information system, especially in the transaction aspect and even more important in the aspect of e-banking. The institutions such as stock exchange, telecoms and other institutions, which information systems collect, process and store important and sensitive data, are using the auditing of information systems on a regular basis. Having in mind that the auditing process requires access and use of different resources, and is implemented by the team of experts, it is possible to conclude that organising and implementing of the audit can be considered as the important project.

According to Avison and Fitzgerald [2], a feasibility study within SSADM (*Structured Systems Analysis and Design Method*) is implemented through four steps:

- **Prepare for the feasibility study** - a step that examines the volume of the project,
- **Define the problem** - a step that compares requirements with the present status,
- **Select feasibility option** – a step that examines available alternatives and selects one,
- **Create feasibility report** – a step of assembling the feasibility report.

Considering the auditing of information systems as a project, it is possible to follow five aspects of the project feasibility hidden behind the acronym TELOS [3]:

- **Technical feasibility** – examines the possibility of applying available technology or if new technology is needed;
- **Economic feasibility** – examines the economic effects or availability of funds to complete the project;
- **Legislative feasibility** – examines potential conflicts between conceptual system and ability of institution to discharge its legal responsibilities;
- **Operational feasibility** – examines the degree of compatibility of the existing procedures and staff skills or new procedures and training are needed; and
- **Schedule feasibility** – examines the ability of in-time implementation of the project.

When considering auditing of information system as the project, these aspects are more flexible compared to the development of information system. However, it is advisable to go through them in order to examine all strengths and weaknesses, opportunities and threats related to the audit. Feasibility study for the auditing process is done in the case of engagement of internal auditor. It is not a part of common audit frameworks but complements it.

2. TELOS Feasibility Aspects

2.1. Technical feasibility

The technical feasibility examines the possibility of applying of available technology or if new technology is needed. The answer it has to provide is – does the actual technology provides satisfactory effects, or it is time to improve, upgrade or completely change it. In the auditing process, implementation of the technology relates to:

- The tools and technologies for the implementation of the audit process, and
- The frameworks for the implementation of the audit process.

Today, IT auditors are using **Computer Aided Audit Tools and Techniques – CATT**. CAAT typically involves basic office software (eg. *MS OFFICE* package) or advanced software tools for statistical analysis (eg. *SPSS*, *SAS*), general audit software (eg. *ACL*, *Arbutus*, *EAS*) as well as business intelligence tools (eg. *SAP* or *Oracle* tools, *Crystal Reports*, *Business Objects*). In the most general sense, CAAT can refer to any computer program used to improve the automation of the audit process at any stage of extraction and analysis of data [4].

This improves the data collection process in the sense that the data collected for audit are adequate data, taken from a right place and at the right time. At the same time, these tools and techniques enable high quality and rapid analysis of collected data, thereby reducing the time required for processing, and thus the time that the auditor requires preparing a report. These tools and techniques are primarily used in financial audit for easy detection of fraud. However, with minor adjustments, these tools and

techniques can be used for auditing information systems. The essence of CAAT tools is to provide a set of functions relating to the preparation, collection and analysis of data, such as:

- tools for querying,
- data stratification,
- sample extraction of data,
- identification the missing sequence,
- statistical analysis,
- calculations,
- identify redundancy, multiple and repeated transactions,
- creating pivot tables,
- cross-tabulation of data, etc.

Using CAATT, the auditor achieves multiple benefits such as:

- it simplifies the audit process,
- comes easier to data,
- the data is prepared in a predetermined format in order to facilitate their processing.

It is very important that these tools are independent of the system that is the subject of the audit. This will enable access to and extraction of data from the system without disrupting its integrity because tools are using and reading only a copy of the data (Read-only copy). Such approach protects data from potential abuse. Also, most of these tools have the possibility to test the data and to document the audit procedures that can be delivered together with an audit report.

CAATT can be classified as [5]:

- *Electronic Working Papers,*
- *Information Retrieval and Analysis),*
- *Fraud Detection,*
- *Network Security,*
- *Electronic Commerce and Internet Security,*
- *Continuous Monitoring,*
- *Audit Reporting,*
- *Database of Audit History,*
- *Computer Based Training,*
- *Time Tracking,*
- Etc.

The audit frameworks provide guidelines for the work of the auditor, guiding the implementation of the audit as systematic (qualitative and quantitative) collecting and processing of data required for the preparation of the audit report. There is a number of worldwide recognised standards and recommendations, but mostly in use are presented in Figure 1.

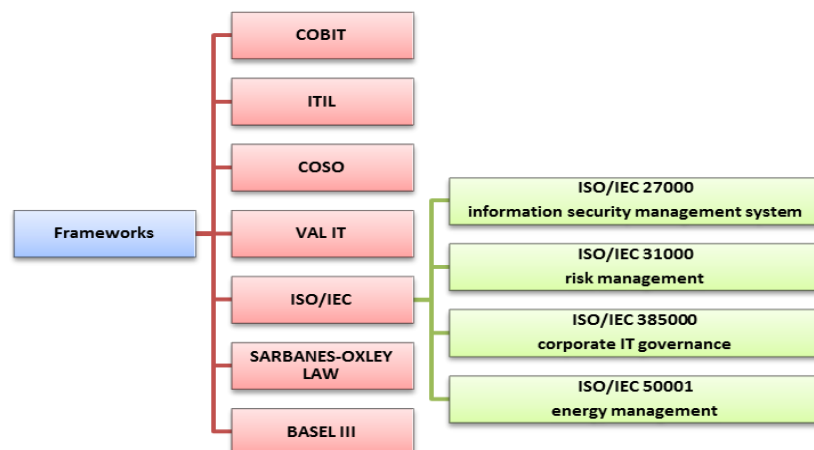


Figure 1. The most used audit frameworks and standards (author)

COBIT (*Control Objectives for Information and Related Technologies*) the most popular framework maintained by Information Systems Audit and Control Association (<http://www.isaca.org>) originating from IT Governance Institute (<http://www.isaca.org/itgi/Pages/default.aspx>) aiming to assist the governance of IT (and information systems). It was published for the first time in 1996 and actual version is number 5 published in 2012, applicable to all kind of companies and institutions [6] COBIT5 defines 7 *enablers*, with more than 300 IT controls grouped in 34 control objectives and 37 processes and 5 domains [7] These five domains of COBIT 5 are following: *Evaluate, Direct and Monitor* – EDM, *Align, Plan and Organise* – APO, *Deliver, Service and Support* – DSS, *Monitor, Evaluate and Assess* – MEA, and *Build, Acquire and Implement* – BAI.

ITIL (*IT Infrastructure Library*) provides a framework of best-practice guidance for IT service management, aiming to harmonise IT services with business needs for facilitating decision making, changes, transformation and growth [8]. The author was *Central Computer and Telecommunications Agency* - CCTA in late 1980-ies (since 2000 changed the name in *UK Office of Government Commerce* - OGC). The first version of ITIL was named GITIM (Government Information Technology Infrastructure Management); the second version was published in 2001 and last and actual version number three was published in 2007 [9]. ITIL is based on top-down approach, organised around the life cycle of services and in five processes described in five volumes [10]: *ITIL Service Strategy*, *ITIL Service Design*, *ITIL Service Transition*, *ITIL Service Operation*, and *ITIL Continual Service Improvement*. Today, this standard is maintained by AXELOS (<https://www.axelos.com>)

There is quite a number of ISO/IEC standards that can be related to the auditing of the information systems, but most important is ISO 27000 family of standards, so-called Information Security Management System – ISMS. The definitions and vocabulary of ISMS are given in ISO 2700:2014 (third version published in 2014). The review of ISO 27000 is presented in Table 1 below.

Val IT framework was published by IT Governance Institute (ITGI) as “*Enterprise Value: Governance of IT Investments, The Val IT Framework 2.0*” and covers three main domains: *Value Governance* – VG, *Portfolio Management* – PM and *Investment Management* - IM [12]

The main aim of Val IT is to assist the company to optimise realisation of values from investments in IT. It includes set of basic principles and number of processes that are defined with the set of key management practices. Val IT was created as a complement to COBIT from the business and financial perspective aiming to improve values coming from investments in IT.

Table 1. Review of ISO/IEC 27000 family of standards (from [11])

Standard's code	Title of the standard
ISO/IEC 27000	<i>Information security management systems — Overview and vocabulary</i>
ISO/IEC 27001	<i>Information security management systems — Requirements</i>
ISO/IEC 27002	<i>Code of practice for information security controls</i>
ISO/IEC 27003	<i>Information security management system implementation guidance</i>
ISO/IEC 27004	<i>Information security management — Measurement</i>
ISO/IEC 27005	<i>Information security risk management</i>
ISO/IEC 27006	<i>Requirements for bodies providing audit and certification of information security management systems</i>
ISO/IEC 27007	<i>Guidelines for information security management systems auditing</i>
ISO/IEC TR 27008	<i>Guidelines for auditors on information security controls</i>
ISO/IEC 27010	<i>Information security management for inter-sector and inter-organizational communications</i>
ISO/IEC 27011	<i>Information security management guidelines for telecommunications organisations based on ISO/IEC 27002</i>
ISO/IEC 27013	<i>Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1</i>
ISO/IEC 27014	<i>Governance of information security</i>
ISO/IEC TR 27015	<i>Information security management guidelines for financial services</i>
ISO/IEC TR 27016	<i>Information security management — Organisational economics</i>

During 1985, the USA accounting and financial associations gathered in alliance named *Committee of Sponsoring Organisations of the Treadway Commission* – COSO with the aim to fund public-private initiative named *National Commission on Fraudulent Financial Reporting* [13]. COSO framework claims that the internal control consists of five interconnected element of which for the audit of information systems the most important is the fourth one [14]: Control Environment, Risk Evaluation, Control Activities, Information and Communication and Monitoring.

Mentioned Sarbanes-Oxley Law and BASEL II and BASEL III recommendations are mostly used in the banking sector. The selection of the framework and the standards shall depend on the depth and domain of the audit, type of institution or organisation and on available funds for performing the audit.

2.2. Economic feasibility

The economic feasibility in auditing of information has aimed to examine the economic effects (positive and negative) of the auditing process without knowing or prejudicing the results of the audit. It is very important to find out the effects and consequences of the performed audit on the client. Namely, economic feasibility should offer a number of scenarios to decision makers on what to do after the audit? This aspect of the feasibility study is the most interesting for organisation's top management and may influence their decision to go into the audit or not.

The auditors, in the preparation phase of the audit and before concluding the final version of the contract, should clearly present the costs against the benefits and volume of the audit. This shall assist decision makers to have a clear picture and motivation to perform the audit. **The main questions that economic feasibility should examine are:**

- What is the level of costs for the auditing and what will be the effects of the audit? Or, what will we get with the auditing and is it beneficial to invest in the auditing?
- What are the indicators and how to make a cost-benefit analysis? How to compare the auditing costs with the corresponding effects achieved with such investment?

To be able to find answers, the economic feasibility should take into consideration following, but not exhaustive, a list of possible auditing costs:

- **Costs of external auditors service** based on to be agreed volume and domain of the audit,
- **Costs that may occur in use of resources** during the auditing process,
- **Costs that may rise in order to train the employees** for facilitation of the audit (if it is needed),
- **Costs of immediate and urgent corrections and interventions** within the system for instant improvement, and
- **Costs related to resolving other (less urgent) audit findings.**

The effects of the audit project can be quantitative or qualitative, but in general, can be divided into two categories:

- **Effects that can be measured** (the indicators are quantified and it is possible to quantify them with the numbers or trends – number of employees, decrease costs, increase of number of services, etc.), and
- **Effect impossible to measure** (the indicators are difficult to quantify or impossible to determine and to assign the number or a value; often they will not be visible immediately upon the implementation of the corrective measures but anytime in lifecycle).

For example, the audit will find that the work of an employee in a certain domain job can be automated within the system and providing the same quality of services using electronic communication between the system and clients. Savings can be calculated on the basis of the hourly rate and multiply it by the number of working hours. The employee works classic 8 work hours per day (or 40 hours working week) which is 168 hours per month. Using the automatized system, the system can improve and extend the working time and provision of services during the whole 24 hours per day, including non-working days. This means that these services will be available not 168 hours per month, but 720 hours monthly. The effective service provision is increased by more than 4 times. Multiplying with an hourly rate, it is easy to find out the direct economic effects.

But there are also some indirect effects, such as increased clients' satisfaction with services offered, operative working time is increased, increased use of services means increased the number of transactions, etc.

Also, the economic feasibility usually uses one or combination of the following methodologies:

- Cost-benefit analysis,
- Payback analysis,
- Return on investment, and
- Net present value.

2.3. *Legislative feasibility*

Legislative feasibility is an important aspect of TELOS. This aspect defines a legal requirement for introduction or implementation of the information system audit. The legal feasibility should provide answers on the legal basis for the audit. In order to obtain such information, the legal feasibility should provide answers to the following questions:

- Is the information system audit obligatory or voluntary?
- What is the frequency of conducting the audit – annually, bi-annually etc.?
- Is the information system audit independent or done together with the internal audit?
- Are there strict legal rules or recommendations imposed or recommended for conducting the audit?
- Are there legal consequences if the audit is not performed and how it can influence security and safety of the information system?

For example, U.S. Government Accountability Office recommends FISCAM methodology described in Federal Information System Controls Audit Manual [15]. The manual provides a methodology for assessing the effectiveness of information system controls and provides the steps in conducting information system audit. The methodology is mandatory and both auditor and audit organisations must comply with it.

International Organisation of Supreme Audit Institutions (INTOSAI) developed own standards with the set of auditing standards based on:

- ISSAI 1 - The Lima Declaration of Guidelines on Auditing Precepts (principle of independence)
- ISSAI 100-400 - INTOSAI Auditing standards (principles of auditor's work) and
- ISSAI 30 - Ethic codex (values and principles of the auditor).

These are INTOSAI key documents that should be considered in planning and conducting the audit of information systems in the public administration.

The importance of information system audit is a necessity in any public administration and should be mandatory. The Supreme Office for the Republic of Srpska Public Sector Auditing in its "Strategy of the Supreme Office for the Republic of Srpska Public Sector Auditing in period 2014-2020" stated the need for intensification of activities related to the information systems audit due to the significant and fast development of ICT [16].

The audit becomes even more important in the case of the decentralised information system of the public administration where the use of various unsecured or partially secured communication channels can jeopardise the work of the system.

Often, due to lack of qualified and skilled auditors, the information system audit is conducted as the part of the internal or financial audit. Therefore, it is necessary to educate and train at least minimal number of information system auditors to secure the quality of the conducted audit and reliable audit report findings. Another solution is contracting of auditors with adequate certification, such as Certified Information System Auditor – CISA. This certification is managed by the Information System and Control Association – ISACA.

2.4. Organisational feasibility

Each public administration institution has strict hierarchical structure. The example of the Ministry of the Government is presented in Figure 2. The top authority is the Minister and as such this position has most of authority and permissions. Depending on complexity and jurisdiction of the Ministry, it can have one or several Deputy Ministers that are in charge for one or number of departments. Each department has Head in charge and civil servants or employees.

There can be other relevant positions (such as Secretary General that can be in the same line as Deputies) in the Ministry, but this is the most common case of an organisation. Although the structure of the organisation is not a key factor for the successful information system audit, such centralised and structured organisation is less complex and enables easier follow up of the reporting and division of authorities. This facilitates check of the control points in the audit process and making conclusion where to intervene for corrective measures, an eventual increase of system efficiency or other audit purposes.

The precise definition of workflows, levels of authorities, division of responsibilities etc. is crucial in the phase of information system development. But at the same time, it is very important for the audit purposes. In that case, the auditor can easily to follow the work process, check the inconsistencies or to search for problems in security and safety.

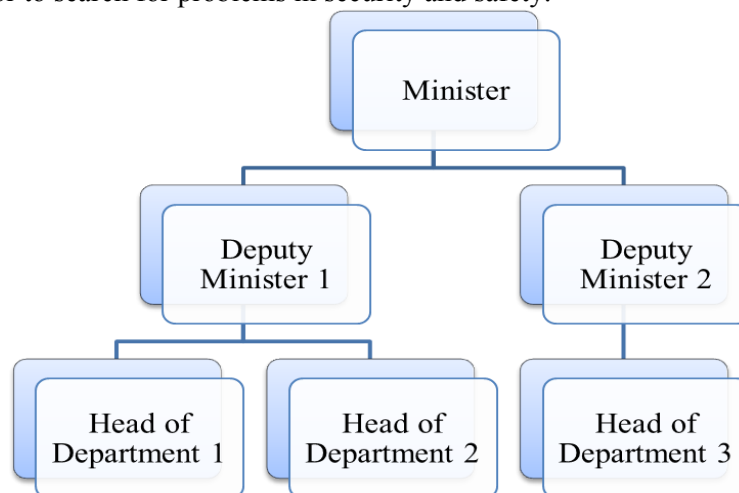


Figure 2. Common structure of the Ministry (author)

2.5. Schedule feasibility

Although it may be an important factor in assessing the overall performance of the feasibility and implementation of information systems, the schedule feasibility is also important from the aspect of information systems auditing.

There are some calculations on the time required for the implementation of each stage of an audit of information systems as shown in Table 2.

Table 2. Audit time consumption per individual phase (from [17])

The phase of the information system audit	Percentage of the total audit time
Preparation and planning	10
Analysis and documentation	10
Collecting audit evidence	25
Analysis and evaluation of the audit evidence	20
Preparation of the audit report	20
Presentation of the audit report	5
Post audit activities	10

Table 2 shows that 45% of the time (planned for the audit) should be invested in data collection and analysis (almost half of the total time), for making the presentation of the report 25% of the time, and 30% for all other audit activities. This means that it is necessary to align all stakeholders in the revision of information systems and to make available the necessary resources.

It is very important to determine when (period, time frame) the core activities of the audit will be conducted - data collection and analysis on the spot. The business processes in the institution during this period will be significantly affected and slowed down and therefore it is necessary to organise the audit in the period when it will minimise the impact of auditors' work on the business. The field work of auditor should be well elaborated and agreed in preparation and audit planning among parties in order to have the desired resources and personnel available.

This will include also the consideration of periods burdened with state or religious holidays, during vacations or in circumstances when an institution is overloaded with the business activities (eg. the organisation and conduct periodic public procurement, immediately prior to preparation of final financial documents at the end of the fiscal year, etc.).

If necessary, the time of the audit can be further extended and for the collection of data with more quality. It is possible that some functionalities of the information system are not in operation at the time of the audit, which prevents quality analysis of all necessary controls and given the possibility of latent system fault in the future. Therefore, it is sometimes necessary to simulate this functionality (if there is no real need for the work at the audit time) in order for the auditor to gain full access to the necessary controls.

3. Conclusion

Each audit of public administration institutions requires good planning and preparation. In order to prepare quality information systems audit, one of the proposed models to do it is using the TELOS methodology.

TELOS methodology recommends the creation of the feasibility study including the five main aspects of the feasibility: technical, economic, legal, organisational and schedule feasibilities.

This paper presented and discussed main questions related to using of TELOS methodology in planning information system audit in the public administration institutions. Moreover, the paper discusses positive effects implementing TELOS methodology.

The objective of the auditor is to highlight the problems of the information system functioning, its deficiencies and potential opportunities for improvement. Therefore, the institution goal should be to implement a quality audit in order to obtain more realistic results and thus managed to prevent potential damage and business losses due to improper functioning of information systems and related business processes and procedures.

In order to obtain real indicators and findings, both parties (auditor and audited institution) should work in close cooperation and with the joint aim to improve the functioning of the overall system. Therefore, it is crucial to consider an auditor more as external assistant and facilitator in the improvement process.

TELOS methodology covers important parts of the complex feasibility study that can in advance point on possible problems for the audit process. Simplicity, ease of use and adaptability to different systems are the main characteristics of this methodology.

References

- [1] Justis R T and Kreigsmann B 1979 The feasibility study as a tool for venture analysis, *Business Journal of Small Business Management* **17**(1) 35-42
- [2] Avison D and Fitzgerald G 2006 *Information Systems Development*, 4th Edition, McGraw-Hill Education, USA
- [3] Hall J A 2011 *Information Technology Auditing and Assurance*, 3rd Edition, South-Western Cengage Learning, USA, pp 187-188
- [4] Stanislav R P 2013 Informaciona bezbednost i primena CAATT alata u IT reviziji, *Pravno-*

- ekonomski pogledi 2*
- [5] *** Portal AuditNet 2017 <https://www.auditnet.org/audit-library/computer-assisted-audit-tools-and-techniques-caatt> (accessed on 12.1.2017)
 - [6] ***ISACA 2016 *COBIT 20th Anniversary* available at <http://www.isaca.org/COBIT/Pages/COBIT-20th-Anniversary.aspx#years> (accessed on 5.8.2016)
 - [7] ***ISACA 2012 *COBIT 5 - A Business Framework for the Governance and Management of Enterprise IT* Rolling Meadows, IL, USA
 - [8] ***Axelos 2016 *What is ITIL® Best practices?* available at <https://www.axelos.com/best-practice-solutions/itil/what-is-itil> (accessed on 1.8.2016)
 - [9] ***ITIL 2016 *Central History of ITIL* available at <http://itsm.fwtk.org/History.htm> (accessed on 1.8.2016)
 - [10] Arraj V 2013 *ITIL®: The basics (White paper)* The APM Group and The Stationery Office
 - [11] ***ISO/IEC 2008 *International standard ISO/IEC 38500:2008 (1st edition)* International Organization for Standardization Geneva Switzerland
 - [12] ***ITGI 2011 *ENTERPRISEVALUE: GOVERNANCE OF IT INVESTMENTS The Val IT Framework 2.0* IT Governance Institute, USA
 - [13] ***COSO 2016 *About us* available at <http://www.coso.org/aboutus.htm>, (accessed on 2.8.2016)
 - [14] ***Ministarstvo finansija Crne Gore 2011 *Priručnik za finansijsko upravljanje i kontrole* Podgorica (available at <http://www.mf.gov.me/pretraga/107135/Prirucnik-za-finansijsko-upravljanje-i-kontrole.html> accessed on 2.8.2016)
 - [15] ***United States Government Accountability Office 2009 *FEDERAL INFORMATION SYSTEM CONTROLS AUDIT MANUAL (FISCAM) GAO-09-232G*, Washington DC, USA (available at <http://www.gao.gov/assets/80/77142.pdf> accessed on 31.3.2017)
 - [16] ***Glavna služba za reviziju javnog sektora Republike Srpske 2013 *Strategija razvoja Glavne službe za reviziju u periodu od 2014. do 2020. godine* Banja Luka, BiH
 - [17] Varga M and Varga V 2011 Usporedba rezultata revizije informacijskih sustava provedenih prema CobiT okviru i uvod u CobiT 5 okvir, *Tehnički glasnik* **5**(1) 35-43