DOI: 10.29202/nvngu/2018-2/14

V. Davidavičienė, Dr. Sc. (Social), Prof.,
I. Aleliūnas, Dr. Sc. (Human.),
J. Sabaitytė, Dr. Sc. (Social)

Vilnius Gediminas technical university, Vilnius, Lithuania, e-mail: vida.davidaviciene@vgtu.lt; irmantas.aleliunas@vgtu.lt; jolanta.sabaityte@vgtu.lt

EUROSAI ITWG MODEL ADOPTION FOR NEW IT AUDIT FRAMEWORK: E-GOVERNMENT CASES

Information and communication technologies have the decisive influence on competitiveness and viability of organization. Efficiency, in general, and the information and communication technologies management processes, in particular, is a key factor in contemporary society and business. However, the success is not guaranteed by implementing new information system or technologies, and a lot of risk and challenges are faced by organizations. To prevent these risks, the IT audit is applied as one of extremely important tools.

Purpose. To evaluate application of existing IT audit methodologies in public sector of Lithuania and the European Commission nowadays and propose augmentation if it is necessary.

Methodology. A systematic literature analysis, benchmarking, observation and structured analysis of the IT audit practice and methodologies. For verifying theoretical model, the empirical data was taken from the Lithuanian Supreme Audit Institution and the Internal Audit Service of the European Commission.

Findings. The analysis of IT audit in governmental institutions revealed that Cobit 3 IT audit model can be implemented nowadays for more efficient IT audit process. During the research the newer methodology of IT audit were taken (Cobit 4.1) for this research and parallels with EUROSAI were drown. Empirical research on EUROSAI WGIT revealed that e-government audit is much wider than project management and quality assurance processes (PO10 and PO11 in COBIT 3.0). Although this research has confirmed that those processes in both institutions still occur most frequently, it has also identified other high risk processes related to IT, such as risk and security management (PO9 and DS5). This work provides basis for the further development of EUSOSAI WGIT e-government audit model taking into account the environmental conditions following the full integration of COBIT5 framework to the proposed methodology. In this case, i.e. paying attention to COBIT5 principle – separation of IT governance domain from IT management domains – we can transform the Cube to the Cuboid. Moreover, as the research revealed some different choices of internal and external auditors, there are new possible areas for research on IT audit in public institutions. This could be the analysis of the differences of internal and external auditors or subjective factors in risk assessment at the initial stages of IT audit.

Originality. A new model of IT audit in e-government systems is proposed on the basis of IT audit methodology Cobit 4.1 and its parallels with EUROSAI, augmented with risk and security management (PO9 and DS5). This provides basis for the further development of EUSOSAI WGIT e-government audit model after full integration of COBIT5 framework to the proposed methodology.

Practical value. Implementation of the proposed model of IT audit in e-government will lead to the decrease in cybercrime, more structured and better managed IT processes in governmental organizations, according to the updated requirements of IT audit methodologies.

Keywords: *IT audit, audit methods, public sector, e-government, IT management, IT risk evaluation, IT audit model*

Introduction. New issues and challenges for public sector organization management, related to information and communication technologies development and worldwide use are caused by various political, economic, cultural, and technical changes and challenges. Cybercrime is one of fast-growing areas of crime. The speed, convenience and anonymity of the Internet are accessible for diverse range of criminal activities that know no borders, either physical or virtual, cause serious harm and pose very real threats to victims worldwide [1]. For increasing economy, efficiency and effectiveness of the own performance, organizations use new solutions of information and communication technologies (like cloud computing solutions, Big data, Open data, etc.), change business process in relation with new possibilities as well as organizational structures. The organizations of public sector become dependent on economy, efficiency, effectiveness, security and compliance of information and communication technologies performance [2]. The rapid growth of the information quantity and importance of IS (information systems) implementation for its management brings new areas of research for the scientists and practitioners. Shift of the focus from information security to cyber security as well raises new questions of research seeking solutions in fields of decisions and performance of public organizations in evaluation of information security, IT (information technologies) auditing, risk management and IS (Information systems) optimization. These factors have direct impact on financial results of organization or can lead to bankruptcy [3]. The IT audit process and suggested models are the main tools for IT security evaluation [4]. So, audit in the area of information and related technologies has become one of the most important and complicated topics of audits being performed by the Supreme Audit Institutions (SAIs) and (or) the Internal

© Davidavičienė V., Aleliūnas I., Sabaitytė J., 2018

audit capabilities (IAC) in public institutions. We can understand this as a natural response to the increasing digitization of the economy and, consequently, in public sector including central and local governments as well. The IT governance and management processes should ensure that organizations protect their data and business assets as well as support mission, financial, and other specific goals. The right balance between IT risk and the value generated by IT should be achieved in a successful organization. While the increasing use of IT has led to improving business efficiency and effectiveness of service delivery, it has also brought with it risks and vulnerabilities associated with computerized databases and business applications, which typically automated working environment [5]. New IT governance and management methods developed by ISACA also create solid methodological basis for IT audit.

The goal of the article is to develop e-government audit model corresponding to contemporary requirements in the public sector based on research in public organizations at national and supranational levels.

The objectives are: to verify EUROSAI ITWG e-government audit model; to adopt e-government audit model to current environment conditions.

The researchers intended to analyses practice of IT audit methodologies (Cobit3, Cobit4.1, COBIT5) model of IT auditing used in public sector organizations in Lithuania and the European Commission (EC) and its relevance in today's environment for identifying key processes and threats.

Analysis of the recent research and publications. Audit in public institutions. A lot of researchers and scientists have been working in the field of IT audit and analyzing various features and different attributes, and issues of cybersecurity [6]. E-government issues themselves were also analyzed by researchers, emphasizing such aspects as e-government inerrability, adoption, quality [7], efficiency [8], and others. Before assessing IT audit in the public sector, and analysing specifics, we are to discuss in short classification and development stages. Mostly, audit is classified according to the following criteria: functional scope and performers, timing, and binding. The following features should be highlighted as functional dependency and institutional dependence. It is worth taking into account the fact that other features will not affect the organization of the audit process, nor will the applicable tests or pro-proceedings after it is accepted. Suggestions proposed by [9] should be considered: e. g. that choice helps reduce information asymmetry and financing frictions when external experts are engaged. In terms of IT audit, these are important features and classification which come from institutional dependence. Such audit types are distinguished as external (independent), internal or public.

The scientific and practical literature focuses on the independent external audit [10]. Moreover, this is confirmed by the fact that the term "audit", although covering both external and internal audits, is usually identified with an independent financial audit in literature, regulations and daily activities. When it comes to other audit types, then it is noted as internal audit, state audit, and so on. So, historically electronic data processing audit has evolved to information systems audit and finally to IT audit [11]. IT audit is a specific audit discipline, which covers all aspects in information systems including IT hardware and software, procedures, people, and information. As organizations move to cloud computing, the Internet of Things, big data, mobile computing, social media and, in addition, information, technology and business converge – new type of audit has evolved recently. ISACA developed Cybersecurity audit Nexus (CSX), a security knowledge platform and professional program [12].

Consequently, after the review of the audit from historic perspective, there follows one conclusion that IT audit is in close connection with other types of audit, as IT is an integral part of any business process in most organizations (Fig. 1). Moreover, IT audit can be defined as a specific type of audit [13]. [5] emphasizes two, more or less, independent approaches to IT audit application areas:

1. Evaluation of internal IT control procedures and environment, as audit of general controls, development controls, application controls.

2. Evaluation of information and related technologies in terms of economy, efficiency, and effectiveness (hereinafter – 3Es), as performance or Value for Money (hereinafter – VFM) audit.

Processes, tools, oversight, and other ways to manage a function in the ICT environment, IT auditors are also referred to as controls. General IT control methods [11] were developed to prevent, detect and correct problems of IT governance, management and security in organizations. Normally, during IT audit auditors evaluate those controls. Evaluation of the audited entity's internal control is an object both of financial and performance (VFM) audits; therefore IT audit is a constituent part of financial and performance (VFM) audits. The objective of audit of IT general controls is to evaluate internal control procedures and environment which cover all information systems of an organization. Audit objectives of IT general controls are related to internal control procedures and internal control environment of entire organization and are applied for all IT systems in enterprise. Audit objectives of application controls are related to data input, processing, out-put and standing data in discrete application. Finally, objectives of IT development controls cover entire lifecycle of project management and development of IT systems. As already

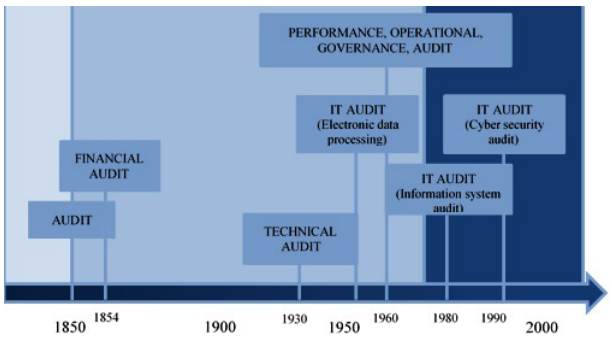


Fig. 1. Audit evolution (created by authors using [12])

stated above, objectives of IT performance (VFM) audit are related to examination of issues connected to information and related technologies in terms of efficiency, economy, and effectiveness. Hence, IT audit can be defined as a separate and specific type of audit and also it can be a part or subtype of any other audit. In case of IT audit in the public sector – peculiarities and specifics such as no profit oriented activities, goals of organization, IT goals and IT controls, should be evaluated and taken into account. Practice and methodologies presented by well-known organizations such as the International organization of supreme audit institutions (INTOSAI) and its regional branches: OLACEFS AFROSAI, ARABOSAI, ASOSAI, PASAI, CAROSAI, and EUROSAI. These organizations overarch the national Supreme Audit Institutions at supranational level. The Institute of Internal Auditors (IIA) – focuses on internal audit. Moreover, this institute provides certification for internal auditors in the public sector (CGAP). Other important organizations in this field are: the International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), the International Federation of Accountants (IFAC), International Information Systems Audit and Control Association (ISACA). In the following chapters, details of IT audit methodology for the research of IT audit processes in the European Union institutions and Lithuanian public sector will be presented.

IT audit methodologies. In order to develop IT audit recommendations for e-government audit model improvement, the existing methodologies, standards and assessment models should be analyzed. Certain auditing standards and code of ethics are the main base of audit approach. Standards of audit are the rules, principles and procedures that define the audit performance and activity. The mostly used standards and procedures are COBIT, ITIL, PRICE2, PMBOK and several standards developed by ISO/IEC.

Following the results of our research and comparative analysis of ITIL, PRINCE2 [14], COBIT [15], ISO 27000 [16], ISO 20000 and other methodologies, we found that COBIT methodology covers full cycle of control objectives (activities) for information and related technologies, and enables a holistic approach taking into account several interacting components of IT governance and management. The COBIT frameworks, provided by IT Governance Institute (ITGI) formed by ISACA encapsulates IT governance and management best practices. They are presented in a structural and logical way and meet different needs of stakeholders in organizations by linking gaps between business and technology. It also provides good basis for performance measurement. This framework provides the structure that links enterprise strategies and objectives to IT processes, IT resources, and information. Moreover, the COBIT is the only methodology from our scope of research which provides solid framework for IT assurance. It started in 1996 as a methodology for IT auditors and from 1998 evolved the scope of this framework to the areas of IT control in version COBIT2. The COBIT3 evolved and covered management needs in the year 2000. In 2005 the versions COBIT4 and COBIT4.1 added summary of process objectives and major tasks, shortlist of major inputs and process deliverables (including where the inputs originate from and where the deliverables go to), list of the most important process activities, identification of those responsible for the activity, RACI chart (those that will be held accountable for its results, and those that need to be consulted and/or informed), and finally – metrics aligned with goals and better link between performance and outcome. So, the previous versions of COBIT were focused on formalization and grouping of LT processes into four domains: planning and organization (PO), acquisition and implementation (AI), delivery and support (DS), and monitoring and evaluation (ME) with clear lines of roles and ownership.

The last COBIT5 version, presented in 2012, deviated from IT control approach, focused on the governance of enterprise IT and added one more domain – to evaluate, direct and monitor (EDM). The COBIT5 product is overarching nowadays and contains five principles and seven enablers.

Each of the examined methodologies has its specificity, even though experts often describe them as universal. So, considering organizational goals, needs and alternative methods the decision can be to use multiple techniques. However, Cobit can be considered as an umbrella methodology for IT audit universe.

The three dimensional view (hereinafter – the Cube) covered by EUROSAI IT WG [17] builds a control space (Fig. 2) where each element corresponds to a group of methods: M (i, j, k). In this function the letters 'i', 'j' and 'k' represent the variables 'audit objects', 'audit types', and 'time perspective', respectively (Fig. 2). This model aggregates theoretical background presented in the previous sections of this article.

E-government audits may focus on the following three types of objects, corresponding to three control levels: management activities, audit, and time oriented attributes.

The first dimension of the Cube presents hierarchy of management activities in three layers: a program as a set of projects (including IT-projects), a project either as a separate IT project or as a project within the program, an information system or information resource maintained to support e-government (hereinafter – IS/IR). The second dimension of the Cube presents three types of audit [17]. Those types have already been discussed above in the text of this article: financial audit, IT audit, and performance (or VFM) audit. The third dimension of the Cube includes three time oriented attributes of the audit in the: pre-implementation, as ex-ante audit, mostly theoretical, as it can have negative influence on auditors' independence, concurrent audit, as continuous audit, usually completed using automated audit procedures and tools, and post-implementation, or ex-post audit.

Later the Cube model deviated from the initial idea, took form of cuboid and is used mostly for content management of the IT audit practices in the European Supreme Audit Institutions.

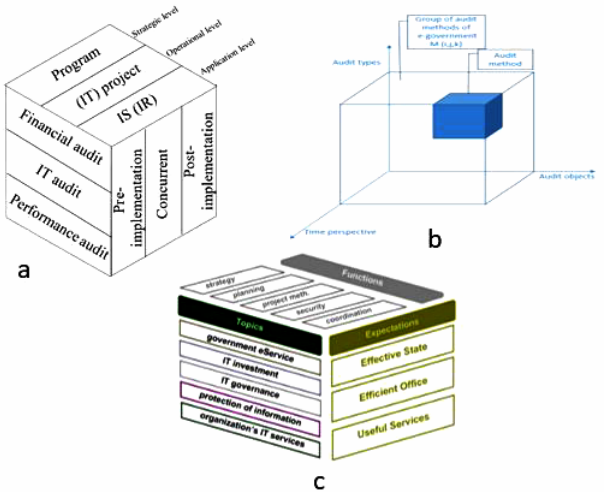


Fig. 2. The Cube of IT audit [17]:

a – control dimensions of e-government; b – correspondence of elements to a group of methods; c – updated control dimensions of e-government

Moreover, audit methods in program, project and IS/IR levels, defined by the EUROSAI IT WG (2004), are already mapped to CobiT 3.0. However, the Cube has become obsolete and re-quires revision, as current and the newest COBIT5 version already exists.

Methodology of the research. The scientist [4, 18] concludes that some research methods are more popular than others in this research area. First top positions are mostly dedicated to: conceptual library research, secondary data analysis, surveys, and case study/interview/semi-structured, and other methods tak-ing not so big part in general sample. [4] emphasizes that multiple methods are often used to capture data from multiple sources as well as to provide a foundation for triangulating data to elicit results from varying perspec-tives in the research of e-governance field. Government audit reports analysis processed by Knapp in 2011 gave an idea for the research.

In this research, for verifying theoretical model, the empirical data are taken from the Lithuanian Supreme Audit Institution within the period 2001–2014 and from the Internal Audit Service of the European Commission within the period 2006–2014. The comparative data analysis used data from official documents.

The data for the research might be presented in two groups. The first group of the documents is a set of audit standards and methodological documents, such as various guide-lines, manuals, handbooks, and others. The sources of those documents are from public organizations – the International Federation of Accountants (IFAC), the Institute of Internal Auditors (IIA), the international professional association focused on IT Governance (ISACA), INTOSAI Professional Standards Committee (INTOSAI PSC) PSC and INTOSAI Working Group on IT Audit (INTOSAI WGITA). The second group of documents includes audit reports prepared on the basis of the first group documents. The sources of this group of documents are data bases in the Lithuanian Supreme Institution where reports of external financial and performance audits in public sector and internal audit reports from internal audit capabilities in public institutions are collected, INTOSAI WGITA data base of performance audit reports, and ISACA ITGI knowledge and insights data base. Quantitative data, such as application frequency of discrete COBIT processes in audits.

The data were treated by statistical methods and techniques. Afterwards, qualitative analyses (data classification and filing) were performed.

Finally, data reduction was done after documentary desk review. The documentary desk review covered verbal (or textual) official documents from the Lithuanian Supreme Audit Institution ant the Internal Audit Service of the European Commission, such as audit reports and working papers. The scope of the research covered all IT audits in those institutions from the defined period of time where COBIT was used as a declared methodology – 18 IT audits from the Lithuanian Supreme Audit Institution and 17 ones from the Internal Audit Service of the European Commission.

The COBIT processes were grouped according to the mapping scheme presented in the Cube. However, in practice auditors used COBIT4.1 version instead of COBIT3, therefore mapping of the Cube to COBIT was tuned to the COBIT4.1 version.

Explanation of scientific results. The result of structural data analysis confirms (Table 1) that the most frequently IT auditors focuses on PO9 (Assess and manage IT risks), PO10 (Manage projects)) and DS5 (Ensure systems security) COBIT4.1 processes.

Hence, risk, project and security management processes make the biggest concern in public organizations. Consequently, as audits were performed using risk based approach, these above mentioned processes also raise biggest risks to the auditees.

The result of the research also shows that PO1 (Define a strategic IT plan), DS4 (Ensure continuous service) and ME3 (Ensure compliance with external requirements) processes also look risky for the auditors in the Lithuanian Supreme Audit Institution. PO4 (Define the IT processes, organization and relationships), AI2 (Acquire and maintain application soft-ware), AI7 (Install and accredited solutions and changes) seem risky for the IT auditors in the Internal Audit Service of the European Commission.

The result of the research also shows that PO3 (Determine technological direction), DS3 (Manage performance and capacity), DS6 (Identify and allocate costs), DS7 (Educate and train users) processes are the least interesting for IT auditors in both institutions.

It should be noted that DS7 (Educate and train users) process was not audited at all. The least interesting processes for IT auditors in the Lithuanian Supreme Audit Institution are identified as PO8 (Manage quality), AI3 (Acquire and maintain technology infrastructure), AI5 (Procure IT resources), DS10 (Manage problems) and DS13 (Manage operations). IT auditors in the Internal Audit Service of the European Commission rarely select PO5 (Manage the IT investment), PO6 (Communicate management aims and direction), PO7

Table 1

Cobit 3 and Cobit4.1 mapped to the EUROSAI cube [15,17]

COBIT 3.0	Program (Strategic)	Project (Operational)	IS/IR (Application)	COBIT 4.1	VK	IAS
PO1 Define a strategic IT plan	x			PO1 Define a strategic IT plan	14	6
PO2 Define the information architecture		x	x	PO2 Define the information architecture	6	3
PO3 Determine technological direction		x	x	PO3 Determine technological direction	2	1
PO4 Define the IT organization and relationships		x		**PO4 Define the IT processes, organization and relationships**	9	7
PO5 Manage the IT investment	x	x	x	PO5 Manage the IT investment	9	1
PO6 Communicate management aims and direction	x	x		PO6 Communicate management aims and direction	8	1
PO7 Manage human resources		x		**PO7 Manage IT human resources**	5	1
PO8 Ensure compliance with external requirements	x	x		ME3 Ensure compliance with external requirements	11	1
PO9 Assess risks	x	x	x	**PO9 Assess and manage IT risks**	10	7
PO10 Manage projects		x		PO10 Manage projects	10	12
PO11 Manage quality		x		PO8 Manage quality	1	5
AI1 Identify automated solutions		x		AI1 Identify automated solutions	5	3
AI2 Acquire and maintain application software		x		AI2 Acquire and maintain application software	9	8
AI3 Acquire and maintain technology infrastructure		x		AI3 Acquire and maintain technology infrastructure	1	4
AI4 Develop and maintain procedures		x				
				AI4 Enable operations and use	3	4
				AI5 Procure IT resources	1	3
AI5 Install and accredit systems		x		AI7 Install and accredited solutions and changes	7	10
AI6 Manage changes		x		AI6 Manage changes	7	6
DS1 Define and manage service levels			x	DS1 Define and manage service levels	6	2
DS2 Manage third-party services			x	DS2 Manage third-party services	8	4
DS3 Manage performance and capacity			x	DS3 Manage performance and capacity	2	1
DS4 Ensure continuous service			x	DS4 Ensure continuous service	12	4
DS5 Ensure systems security			x	DS5 Ensure systems security	13	9
DS6 Identify and allocate costs			x	DS6 Identify and allocate costs	2	0
DS7 Educate and train users			x	DS7 Educate and train users	0	0
DS8 Assist and advise customers			x	DS8 Manage service desk and incidents	2	3
DS9 Manage the configuration			x	DS9 Manage the configuration	4	5
DS10 Manage problems and incidents			x	DS10 Manage problems	0	3
DS11 Manage data			x	DS11 Manage data	4	5
DS12 Manage facilities			x	**DS12 Manage physical environment**	5	3
DS13 Manage operations			x	DS13 Manage operations	0	3
M1 Monitor the processes	x	x	x	**ME1 Monitor and evaluate IT performance**	5	2
M2 Assess internal control adequacy		x	x	**ME2 Monitor and evaluate internal control**	9	1
M3 Obtain independent assurance		x	x			
M4 Provide for independent audit		x	x			
				ME4 Provide IT Governance	4	2

(Manage IT human resources), ME2 (Monitor and evaluate internal control) and ME3 (Ensure compliance with external requirements.

In some cases, significant differences are found in the frequency of analyzed processes by IT auditors in those different institutions. As an example, the Lithuanian Supreme Audit Institution rarely focuses on PO8 (Manage quality) and AI3 (Acquire and maintain technology infrastructure) process, whereas IT auditors in the Internal Audit Service of the European Commission pay great attention to these processes.

However, IT auditors in the Internal Audit Service of the European Commission rarely audit PO5 (Manage the IT investment) and ME2 (Monitor and evaluate internal control) processes, while IT auditors in the Lithuanian Supreme Audit Institution pay great attention to these processes. Consequently, we can make presumption and raise some hypotheses related to the differences between internal and external audit in public institutions for the future research. Note. COBIT 3.0 processes in bold slightly changed their naming after update of the framework to the version COBIT 4.1. COBIT 3.0 processes underlined completely changed place or naming in version COBIT 4.1.

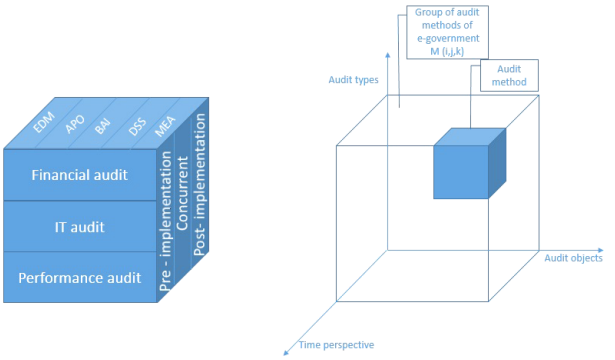
Table 1 reflects the idea that auditing e-government projects and programs should not be limited and reduced to some COBIT domains or CobiT standard processes, such as PO10 (Project management) and PO11 (Quality management). Empirical data fully confirms this hypothesis.

Updated e-government model. As ISACA presented new versions of COBIT, the next step in our research was to update EUROSAI WGITA methodology accordingly. The first update to the version COBIT 4.1 was trivial (Table 1). However, COBIT5 introduced updated approach to the artefacts of IT governance and management. Furthermore, new EDM (Evaluate, Direct and Monitor) domain of processes was introduced in this version. The mapping of EUROSAI WGITA methodology keeps the same table format (Table 2).

However, COBIT5 is based on new principles – covering the enterprise End-to-end, Applying a Single, Integrated Framework, and Enabling a Holistic Approach – this upgrade allows full integration of COBIT5 to EUROSAI WGIT e-government model. In this case the Cube should be transformed to the rectangular cuboid (the Cuboid), as one of the dimensions consists five levels, corresponding to COBIT5 process groups – EDM, APO, BAI, DSS, MEA (Fig. 3).

As we can see in Table 2, COBIT5 has a different number of processes. But the most significant change is related to the different problem – the groups of COBIT5 domains correspond to the second and third dimension of the Cube in EUROSAI WGITA methodology, but the first dimension of the Cube was reshaped because COBIT5 also covers governance domains.

So, we have presentation of e-government audit in the new Cuboid model, which segregates governance and management processes. Consequently, IT auditors could have theoretical background for the wider scope of IT audits. This Cuboid can be tested in the future, as



a *b*

Fig. 3. Proposed model of e-government audit:
a – updated Cuboid of IT audit; b – correspondence of elements to a group of methods

soon as enough empirical data can be collected. So, it can be a good methodological basis for the research in the future.

Conclusions. In the article theoretical aspects of IT audit in governmental institutions were analyzed with regard to possibilities of IT audit model use. The verification revealed that Cobit 3 IT audit model can be implemented in IT audit analysis nowadays. During the research the newer methodology of IT audit was taken (Cobit 4.1) for this research and parallels with EUROSAI were drown. This action enabled to prove that the Cube methodology may be adopted in the future for higher versions of Cobit (e.g. Cobit 5.0).

Empirical research of EUROSAI WGIT revealed that e-government audit is much wider than project management and quality assurance processes (PO10 and PO11 in COBIT 3.0). Although this research confirmed that those processes in both institutions are still the most frequent, it also identified other high risk processes related to IT, such as risk and security management (PO9 and DS5).

The article provides basis for the further development of EUSOSAI WGIT e-government audit model to current environment conditions following the full integration of COBIT5 framework to the proposed methodology. In this case, i.e. paying attention to COBIT5 principle – separation of IT governance domain from IT management domains – we can transform the Cube to the Cuboid.

Moreover, as the research revealed some different choices of internal and external auditors, there are new possible areas for research of IT audit in public institutions. Those areas could cover analysis of the differences of internal and external auditors or subjective factors in risk assessment at the initial stages of IT audit.

References.

1. INTERPOL, 2016. Cybercrime / Cybercrime / Crime areas / Internet / Home – INTERPOL [online]. Available at: <https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime> [Accessed 16 September 2017].

2. Arduini, D., Denni, M., Lucchese, M., Nurra, A. and Zanfei, A., 2013. The role of technology, organiza-

Table 2

Cobit 5 mapped to the EUROSAI cube [15,17]

Domain	COBIT 5 process	Program (Strategic)	Project (Operational)	IS/IR (Application)
Evaluate, Direct and Monitor (EDM)	EDM01. Ensure governance framework setting and maintenance	N/S		
	EDM02. Ensure benefits delivery	N/S		
	EDM03. Ensure risk optimization	N/S		
	EDM04. Ensure resource optimization	N/S		
	EDM05. Ensure stakeholder transparency	N/S		
ALIGN, PLAN AND ORGANISE (APO)	APO01. Manage the IT management framework	x		
	APO02. Manage strategy	x		
	APO03. Manage enterprise architecture	x		
	APO04. Manage innovation	x		
	APO05. Manage portfolio	x		
	APO06. Manage budget and costs	x		
	APO07. Manage human resources	x		
	APO08. Manage relationships	x		
	APO09. Manage service agreements	x		
	APO10. Manage suppliers	x		
	APO11. Manage quality	x		
	APO12. Manage risk	x		
	APO13. Manage security	x		
BUILD, ACQUIRE AND IMPLEMENT (BAI)	BAI01. Manage programs and projects		x	
	BAI02. Manage requirements definition		x	
	BAI03. Manage solutions identification and build		x	
	BAI04. Manage availability and capacity		x	
	BAI05. Manage organizational change enablement		x	
	BAI06. Manage changes		x	
	BAI07. Manage change acceptance and transitioning		x	
	BAI08. Manage knowledge		x	
	BAI09. Manage assets		x	
	BAI10. Manage configuration		x	
DELIVER, SERVICE AND SUPPORT (DSS)	DSS01. Manage operations			x
	DSS02. Manage service requests and incidents			x
	DSS003. Manage problems			x
	DSS04. Manage continuity			x
	DSS05. Manage security services			x
	DSS06. Manage business process controls			x
MONITOR, EVALUATE AND ASSESS (MEA)	MEA01. Monitor, evaluate and assess performance and conformance	x		
	MEA02. Monitor, evaluate and assess the system of internal control	x		
	MEA03. Monitor, evaluate and assess compliance with external requirements	x		

tion and contextual factors in the development of e-Government services: An empirical analysis on Italian Local Public Administrations. *Structural Change and Economic Dynamics*, 27, pp. 177–189.
3. Vande Putte, D. and Verhelst|, M., 2013. Cyber crime: can a standard risk analysis help in the challenges facing business continuity managers? *Journal of Business Continuity & Emergency Planning,* 7, pp. 126–137.
4. Joseph, RC., 2013. A structured analysis of e-government studies: Trends and opportunities. *Government Information Quarterly*, 30, pp. 435–440.
5. INTOSAI WGITA II., 2014. WGITA – IDI *Handbook on IT audit for Supreme Audit Institutions* [online]. Available at: < http://icisa.cag.gov.in/resource_files/c60986ef8dd5d4f658df077c1b5dceb7.PDF> [Accessed 05 April 2017].
6. Xu, K., Wang, F. and Jia, X., 2016. Secure the Internet, one home at a time. *Security and Communication Networks*, 9, pp. 3821–3832.
7. Gupta, KP., Bhaskar, P. and Singh, S., 2016. Critical Factors Influencing E-Government Adoption in India: *Journal of Information Technology Research (JITR)*, 9, pp. 28–44.
8. Gable, M., 2015. Efficiency, Participation, and Quality: Three Dimensions of E-Government? *Social Science Computer Review*, 33, pp. 519–532.
9. Kausar, A., Shroff, N. and White, H., 2016. Real effects of the audit choice. *Journal of Accounting and Economics*, 62, pp. 157–181.
10. Pike, B.J., Chui, L., Martin, K.A. and Olvera, R.M., 2016. External Auditors' Involvement in the Internal Audit Function's Work Plan and Subsequent Reliance Before and After a Negative Audit Discovery. *Auditing: A Journal of Practice & Theory*, 35, pp. 159–173.
11. Weber, 2016. *Information Systems: Control & Audit* [online]. Available at: <https://www.amazon.in/Information-Systems-Control-AuditWeber/dp/8178086018/ref=sr_1_16?s=books&ie=UTF8&qid=1479989411&sr=116&keywords=information+system+audit> [Accessed 14 March 2017].
12. ISACA, 2016. Cybersecurity Nexus – Cyber Security Training – Security Certification – CSX | ISACA.
13. Mahlknecht, A., Abuzahra, M.E., Piccoliori, G., Enthaler, N., Engl, A. and Sönnichsen, A., 2016. Improving quality of care in general practices by self-audit, benchmarking and quality circles. *Wiener klinische Wochenschrift*, 128, pp. 706–718.
14. PRINCE2 TSO. 2016. Published of behalf of the Office of Government Commerce.
15. ISACA, 2016. COBIT 5: A Business Framework for the Governance and Management of Enterprise IT [online]. Available at: <http:// www.isaca.org/cobit/pages/default.aspx> [Accessed 5 August 2017].
16. International Organization for Standardization, 2013. ISO/IEC 27002:2013 – Information technology – Security techniques – Code of practice for information security controls [online]. Available at: <https://www.iso.org/standard/ 54533.html> [Accessed 21 February 2018].
17. EUROSAI IT working group, 2016. *EUROSAI IT WG. CUBE* [online]. Available at: <http://eurosai-it.org/czysta/cube> [Accessed 21 May 2017].
18. Osman, I.H., Anouze, A.L., Irani, Z., Al-Ayoubi, B., Lee, H., Balcı, A., Medeni, T.D. and Weerakkody, V., 2014. COBRA framework to evaluate e-government services: A citizen-centric perspective. *Government information quarterly*, 31, pp. 243–256.

Адаптація моделі EUROSAI ITWG для нової структури IT-аудита: приклад електронного уряду

В. Давідавічієнė, І. Алелійнас, І. Сабайтіте
Вільнюський технічний університет імені Гедімінаса, м. Вільнюс, Литва, e-mail: vida.davidaviciene@vgtu.lt; irmantas.aleliunas@vgtu.lt; jolanta.sabaityte@vgtu.lt

Інформаційні й комунікаційні технології мають вирішальний вплив на конкурентоспроможність організації. Ефективність у цілому, та особливо у процесах управління інформаційно-комунікаційними технологіями, є одними із ключових факторів у сучасному суспільстві й бізнесі. Проте успіх не гарантується одним тільки впровадженням нової інформаційної системи або технологій, при впровадженні системи організації стикаються з ризиками. Для запобігання таких ризиків використовується IT-аудит як один із надзвичайно важливих інструментів.

Мета. Оцінити застосування існуючих методологій IT-аудиту в державному секторі Литви та Європейської комісії в даний час і запропонувати поліпшення, якщо це необхідно.

Методика. Систематичний аналіз літератури, порівняльний аналіз, спостереження й структурований аналіз практики й методологій IT-аудиту. Для перевірки теоретичної моделі емпіричні дані були взяті з Вищої ревізійної установи Литви й Служби внутрішнього аудиту Європейської комісії.

Результати. Аналіз IT-аудиту в урядових установах показав, що на даний час модель IT-аудиту Cobit 3 може бути реалізована для більш ефективного процесу аудиту. Під час дослідження була використана нова методологія IT-аудиту (Cobit 4.1) і паралель з EUROSAI була проведена. Емпіричні дослідження EUROSAI WGIT показали, що аудит електронного уряду набагато ширше, ніж процеси управління проектами й забезпечення якості (PO10 і PO11 в COBIT 3.0). Однак це дослідження підтвердило, що ці процеси в обох установах як і раніше найбільш часто зустрічаються, але дослідження також виявило інші процеси високого ризику, пов'язані з IT, такі як управління ризиками та безпекою (PO9 і DS5). У роботі формується основа для подальшого розвитку моделі аудиту електронного уряду EUSOSAI WGIT, беручи до уваги умови навколишнього середовища, після повної інтеграції моделі COBIT5 із запропонованою методологією. У цьому випадку, звертаючи увагу на принцип COBIT5 – розділення домену урядових IT і доменів управління IT – з'являється можливість трансформувати куб у Cuboid. Більш того, оскільки дослі-

дження показало, що існують відмінності між внутрішніми й зовнішніми аудиторами, з'являються нові можливості для дослідження IT-аудиту в державних установах. Це може бути аналіз відмінностей між внутрішніми й зовнішніми аудиторами або аналіз суб'єктивних чинників в оцінці ризику на початкових етапах аудиту IT.

Наукова новизна. Нова модель IT-аудиту в системах електронного уряду пропонується на основі методології аудиту IT Cobit 4.1 і її паралелей з EUROSAI, доповненої управлінням ризиками й безпекою (PO9 і DS5). Це забезпечує основу для подальшого розвитку EUSOSAI WGIT модель електронного уряду після повної інтеграції основи COBIT5 у запропоновану методологію.

Практична значимість. Упровадження запропонованої моделі IT-аудиту в електронному уряді призведе до скорочення кіберзлочинності, більш структурованих і поліпшених керованих IT-процесів в урядових організаціях відповідно до оновлених вимог методологій аудиту IT.

Ключові слова: *аудит IT, методи аудиту, державний сектор, електронний уряд, управління IT, оцінка IT-ризиків, модель аудиту IT*

Адаптация модели EUROSAI ITWG для новой структуры IT-аудита: пример электронного правительства

В. Давидавичиенė, И. Алелиūнас, И. Сабайтите

Вильнюский технический университет имени Гедиминаса, г. Вильнюс, Литва, e-mail: vida.davidaviciene@vgtu.lt; irmantas.aleliunas@vgtu.lt; jolanta.sabaityte@vgtu.lt

Информационные и коммуникационные технологии оказывают решающее влияние на конкурентоспособность организации. Эффективность в целом, и особенно в процессах управления информационно-коммуникационными технологиями, является одними из ключевых факторов в современном обществе и бизнесе. Однако успех не гарантируется одним только внедрением новой информационной системы или технологий, при внедрении системы организации сталкиваются с рисками. Для предотвращения таких рисков используется IT-аудит как один из чрезвычайно важных инструментов.

Цель. Оценить применение существующих методологий IT-аудита в государственном секторе Литвы и Европейской комиссии в настоящее время и предложить улучшения, если это необходимо.

Методика. Систематический анализ литературы, сравнительный анализ, наблюдение и структурированный анализ практики и методологий IT-аудита. Для проверки теоретической модели эмпирические данные были взяты из Высшего ревизионного учреждения Литвы и Службы внутреннего аудита Европейской комиссии.

Результаты. Анализ IT-аудита в правительственных учреждениях показал, что в настоящее время модель IT-аудита Cobit 3 может быть реализована для более эффективного процесса аудита. Во время исследования была использована новая методология IT-аудита (Cobit 4.1) и параллель с EUROSAI была проведена. Эмпирические исследования EUROSAI WGIT показали, что аудит электронного правительства намного шире, чем процессы управления проектами и обеспечения качества (PO10 и PO11 в COBIT 3.0). Однако это исследование подтвердило, что эти процессы в обоих учреждениях по-прежнему наиболее часто встречаются, но исследование также выявило другие процессы высокого риска, связанные с IT, такие как управление рисками и безопасностью (PO9 и DS5). В работе формируется основа для дальнейшего развития модели аудита электронного правительства EUSOSAI WGIT, принимая во внимание условия окружающей среды, после полной интеграции модели COBIT5 с предлагаемой методологией. В этом случае, обращая внимание на принцип COBIT5 – разделение домена правительственных IT от доменов управления IT – появляется возможность трансформировать куб в Cuboid. Более того, поскольку исследование показало, что существуют различия между внутренними и внешними аудиторами, появляются новые возможности для исследования IT-аудита в государственных учреждениях. Это может быть анализ различий между внутренними и внешними аудиторами или анализ субъективных факторов в оценке риска на начальных этапах аудита IT.

Научная новизна. Новая модель IT-аудита в системах электронного правительства предлагается на основе методологии аудита IT Cobuit 4.1 и ее параллелей с EUROSAI, дополненной управлением рисками и безопасностью (PO9 и DS5). Это обеспечивает основу для дальнейшего развития EUSOSAI WGIT модель электронного правительства после полной интеграции основы COBIT5 в предлагаемую методологию.

Практическая значимость. Внедрение предлагаемой модели IT-аудита в электронном правительстве приведет к сокращению киберпреступности, более структурированных и улучшенных управляемых IT-процессов в правительственных организациях в соответствии с обновленными требованиями методологий аудита IT.

Ключевые слова: *аудит IT, методы аудита, государственный сектор, электронное правительство, управление IT, оценка IT-рисков, модель аудита IT*

Рекомендовано до публікації докт. техн. наук A. V. Vasiliauskas. Дата надходження рукопису 23.01.17.