

ONE CONCEPT FOR IT AUDIT

Dalibor Radovanović

Singidunum University, Serbia

Tijana Radojević

Singidunum University, Serbia

Saša Adamović

Singidunum University, Serbia

Marko Šarac

Singidunum University, Serbia

Abstract

This paper explains the concept of information systems audit, which is the process of gathering and evaluating evidence based on which one can evaluate the performance of IT systems. It is necessary to determine whether the operation of information systems in the function of preserving the property and maintain data integrity. Revision information system is imposed as an imperative for successful business. One of the methodologies for auditing information systems is COBIT, which provides guidelines on what can be done in an organization in terms of control activities, measurement and documentation of processes and operations.

Keywords: IT audit, IT governance, Cobit.

INTRODUCTION

Critical element important for the survival and success of the organization is effectively managing information and communication technology (ICT), which is reflected in the increase depending on the information and their associated systems, that increase vulnerability and threats to a wide range of ICT technology.

IT audit is a process of gathering and evaluating evidence based on which one can evaluate the performance of IT systems, i.e. to determine whether the operation of information systems in the function of preserving the property and maintain data integrity. It is also necessary to determine whether the information system enables the effective implementation of business objectives and whether the use of system resources in an effective and efficient manner. IT audit today is a modern and advisory function, "right hand" that helps the management of corporate IT Governance. Also, a procedure which assesses whether the information technology act in accordance with business objectives, the extent to effectively and efficiently supports the goals of business and what is the practice (maturity) management and control of information systems at various hierarchical levels. There are several methodologies and stan-

dards that deal with this problem: COBIT, ITIL, COSO, ISO 17799 and ISO 9000.

COBIT

COBIT is a worldwide accepted standard in which the prescribed areas and individual controls for corporate governance, informatics and related IT processes. Authors COBIT framework are non-profit organization ISACA and ITGI. It combines business and IT goals, providing the ability to monitor the maturity of the information metric system. COBIT provides management can optimize IT resources such as applications, information, infrastructure and people, and provides instructions that are the product of consensus knowledge of many experts and the product is good practice, applicable in any organization.

COBIT consists of 34 key business control processes describing each process model of maturity. It contains over 300 detailed IT controls. The primary control objectives are divided into four domains:

- Planning and Organization - PO, includes processes for planning and design organization in the function of achievement of business goals of the organization. This domain includes risk assessment.

- Acquisition and Implementation - AI, includes processes related to the acquisition and development of IT solutions and manages changes of these solutions throughout the time.
- Delivery and Support - DS, includes the processes that affect the actual delivery of IT services to organization. This domain includes the processes for manage problems and incidents; manage security and other processes that affect the performance of IT.
- Monitoring and Evaluation - ME, includes processes for regular review of IT processes and their successfulness in the function of achievement of relevant IT controls objectives.

For each of the key business and IT processes COBIT defines and provides:

- Maturity models
- Critical success factors – CSF
- Key goal indicators – KGI
- Key performance indicators – KPI
- RACI chart
- Control objectives and control tests.

By using COBIT methodology management and corporate structures is easy to determine which of these processes and in what extent are important. From the point of control and information systems audit COBIT determines 18 applications and 6 of process controls. Assessments of maturity are based on the famous CMM model, only that in COBIT model marks are very detailed described and explained for each process. Assessment of maturity of IT governance processes are in the range of 0 to 5:

- **0** - *There are no processes*, process of IT governance do not exist. Management did not recognize the importance of this concept; the decisions on investments in IT are uncontrolled, from case to case ('ad hoc'), outside the system supervision and risk assessment and are completely in the hands of individuals.
- **1** - *Initial processes*, management is not aware of the importance of IT governance, although there are no formal procedures, management and over

sight of information technology is mostly based on individual and uncontrolled based, and actions are taken on case by case basis. There are no standards, nor corporate rules, nor obligations and responsibilities regarding this issue. Management generally is not aware of the importance of IT risk. IT governance and its performance measurement are processes that are carried out only within the IT department, and management is passive, uneducated and not aware of this matter.

- **2** - *Repeatable processes*, IT governance processes exist, but it is uncoordinated and mainly initiated by IT department or some other operating level. It often happens that many people perform the same task (segregation of duties issue); there is no system's supervision, coordination, or standardized procedures. The responsibility is left to individuals; corporate policies do not exist or are not presented to employees.
- **3** - *Defined processes*, IT governance procedures are prescribed and documented, and constantly improved through formal trainings and education. Procedures and corporate rules, although neither formally exists, are not sophisticated, mature nor customized to organization business. They only represent the formalization of existing procedures. Although procedures exist, the responsibility for its execution is on the individuals, and having in mind that there is no system supervision, it is unlikely that one can detect anomalies regarding this matter.
- **4** - *Managed processes*; except corporate policies and procedures exist, it also is possible to constantly monitor their execution, to measure their performance and to take necessary corrections in accordance with needs. Processes and activities are continuously improved. Very sophisticated IT governance objectives closely aligned with the business objectives are being set. Using of current methods and frameworks in performance measurement and IT audit is required.

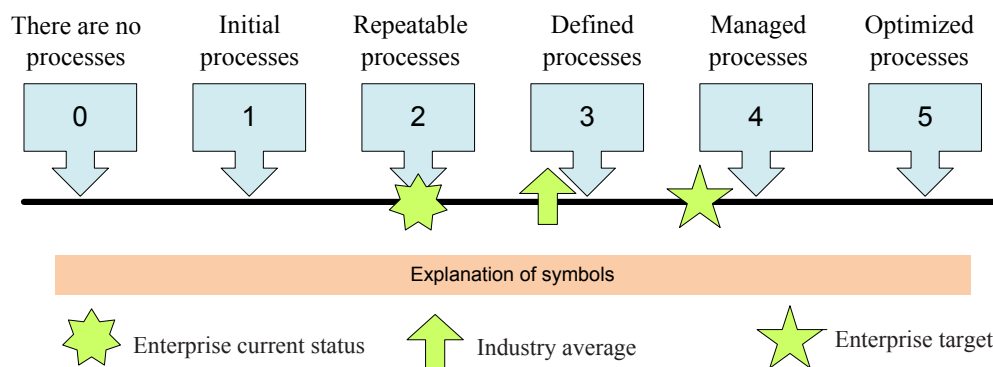


Fig. 1. Graphic display of maturity assessment process

- **5 - Optimized processes**, IT governance processes are brought to the optimal level and the company is a leader in the area. Performance and efficiency of IT as a business function is constantly measured, and the results are compared with best practice and other organizations. Complete transparency in IT governance; corporate bodies have actual supervision over information technology through a series of formal mechanisms. Information technology is used in a strategic purpose, as key business resource and information activities (investments, projects, risks, etc.) are optimally functioning align with the real business priorities.

To assess the results of the maturity of management processes were usable in a comprehensive way, when your need to control structures of organizations are presented graphically as in Figure 1. In such a manner shown in the company's management can easily see the situation in which there are processes in their company. Most important thing to notice is the average grade of maturity in the industry in which they are, and compare it with their own. Management companies may in such a graphic presentation see, in which direction should continue with the improvement process, i.e., they see the goal which must aspire

To meet business objectives, information needs to be in accordance with a specific control criteria that are consistent with the COBIT framework and business information needs. COBIT framework highlights seven different criteria in relation to business requirements, and overlaps each other:

- **Effectiveness** - Information should be relevant and important to the business process. It is necessary to deliver on time, accurate, consistent and usable way.
- **Efficiency** - Information must be provided through the optimal use of resources.
- **Confidentiality** - Sensitive information must be protected from unauthorized disclosure.
- **Integrity** - Information should be accurate, complete, correct and in accordance with business values and expectations.
- **Availability** - Information should be available when required by the business process, as at present, so in the future. Must maintain the necessary resources.
- **Compliance** - the information must be in accordance with the laws, regulations and contractual arrangements that are the subject of business processes, and internal policies.
- **Reliability** - Appropriate information must be provided to management for management purposes and in order to achieve business goals.

COBIT CONTROL OBJECTIVES

COBIT methodology is used a lot in recent years by many organizations, approved and tested by experts around the world.

In Table 1 are shown COBIT control objectives and methodology of information criteria that support the control objectives. COBIT control objectives are designed for information technology auditors, and for each control objective is defined the importance of its implementation, which can be large, medium or small.

The importance of each target letter was

marked importance, a large letter M, S or M. For the information of each target criteria defined roles, which can be demonstration or

secondary, depending on which information is most important criterion, which is less important.

Table 1. COBIT Control Objectives

LABEL	COBIT CONTROL OBJECTIVES	IMPORTANCE	Information Criteria							IT Resources			
			Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability	Applications	Information	Infrastructure	People
PO - PLAN AND ORGANISE													
PO1	Define a strategic IT plan	H	P	S						✓	✓	✓	✓
PO2	Define the information architecture	L	S	P	S	P				✓	✓		
PO3	Determine technological direction	M	P	P						✓		✓	
PO4	Define the IT processes, organization and relationships	L	P	P									✓
PO5	Manage the IT investment	M	P	P					S	✓		✓	✓
PO6	Communicate management aims and direction	M	P					S			✓		✓
PO7	Manage IT human resources	L	P	P									✓
PO8	Manage quality	M	P	P		S			S	✓	✓	✓	✓
PO9	Assess and manage IT risks	H	S	S	P	P	P	S	S	✓	✓	✓	✓
PO10	Manage projects	H	P	P						✓		✓	✓
AI - ACQUIRE AND IMPLEMENT													
AI1	Identify automated solutions	M	P	S						✓		✓	
AI2	Acquire and maintain application software	M	P	P		S			S	✓			
AI3	Acquire and maintain technology infrastructure	L	S	P		S	S					✓	
AI4	Enable operation and use	L	P	P		S	S	S	S	✓		✓	✓
AI5	Procure IT resources	M	S	P				S		✓	✓	✓	✓
AI6	Manage changes	H	P	P		P	P		S	✓	✓	✓	✓
AI7	Install and accredit solutions and changes	M	P	S		S	S			✓	✓	✓	✓
DS - DELIVER AND SUPPORT													
DS1	Define and manage service levels	M	P	P	S	S	S	S	S	✓	✓	✓	✓
DS2	Manage third-party services.	L	P	P	S	S	S	S	S	✓	✓	✓	✓
DS3	Manage performance and capacity	L	P	P			S			✓		✓	
DS4	Ensure continuous service	M	P	S			P			✓	✓	✓	✓
DS5	Ensure systems security	H			P	P	S	S	S	✓	✓	✓	✓
DS6	Identify and allocate costs	L		P					P	✓	✓	✓	✓
DS7	Educate and train users	L	P	S									✓
DS8	Manage service desk and incidents	L	P	P						✓			✓
DS9	Manage the configuration	M	P	S			S		S	✓	✓	✓	
DS10	Manage problems	M	P	P			S			✓	✓	✓	✓
DS11	Manage data	H				P			P		✓		
DS12	Manage the physical environment	L				P	P					✓	
DS13	Manage operations	L	P	P		S	S			✓	✓	✓	✓
ME - MONITOR AND EVALUATE													
ME1	Monitor and evaluate IT performance	H	P	P	S	S	S	S	S	✓	✓	✓	✓
ME2	Monitor and evaluate internal control	M	P	P	S	S	S	S	S	✓	✓	✓	✓
ME3	Ensure compliance with external requirements	H						P	S	✓	✓	✓	✓
ME4	Provide IT governance	H	P	P	S	S	S	S	S	✓	✓	✓	✓

Control goals may have more primary or secondary information criteria within a goal in the table are marked initial letters of the role (importance), P or S.

Also, for each goal are defined and the IT resources needed for a particular purpose. Resources can be applications, information, infrastructure and people. Objectives can be

assigned all the resources, as is the case with the control order PO9, which defines the management and assessment of risk, or may be assigned only one resource, the control objective PO7.



Fig. 2. Total numbers of activities under the control of methodology goals COBIT

Each control objective within COBIT methodology consists of a number of defined activities. Number of activities under the control objectives is not constant.

There are a total of 197 defined activities under the four domains. Figure 2 shows the number of individual activities for each control

objective within COBIT methodology. Total number of activities in the fields:

- Planning and organization - defined 52 activities;
- Acquisition and implementation - defined 42 activities;
- Delivery and support - defined 80 activities;
- Monitoring and evaluation of success - defined 23 activities.

CONCLUSION

An audit of information systems in a short period of time has passed through a dynamic development path. Her original role was support for the audit of financial statements. Today, the audit of information systems is increasingly an essential analytical link the corporate IT governance process. Represent a bridge between management and information technology. It is important component of the concept of corporate IT governance. Use it to evaluate whether the information technology act in accordance with business objectives, to what extent effective and appropriate support business objectives and what the practice (maturity) management and control information system at various hierarchical levels.

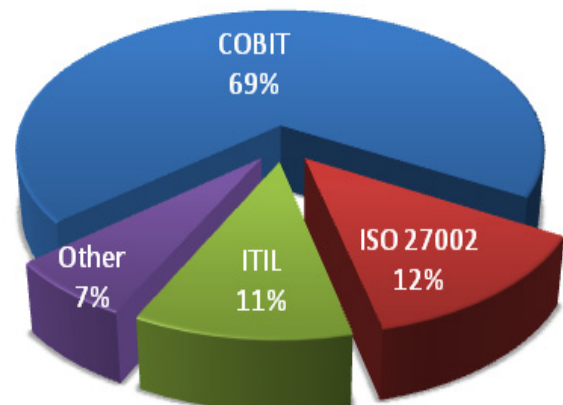


Fig. 3. Standards and frameworks that are used for planning IT audit activity

In the period from 1 June to 31 July 2010 Company Ernst & Young conducted a survey which included 1865 companies from 61 countries, covering all major industries. This research belongs to the group of the oldest and most respected researches of this type. It provides a comparison of companies in respect

of major areas of information security and IT governance.

COBIT are increasingly popular for planning IT audit activity (Fig. 3) and are adopted by 69 percent of respondents. These frameworks deliver a structured approach to planning and focus the IT audit on the business and technological risks of the organization.

The final result of these procedures is information systems auditor's report, which according to the areas of analysis, based on COBIT methodology consists of the following steps:

- Analysis of state (maturity) the application of information systems and technology in business to the observed areas;
- Assessment of business risks arising from the current situation;
- Recommendations to improve the management of this condition.

REFERENCE

[1] Brand, K., & Boonen, H. (2008). IT Govern

ance based on Cobit 4.1 - A Management Guide. Van Haren Publishing.

[2] Cannon, D. L. (2008), CISA Certified Information Systems Auditor Study Guide. Sybex.

[3] Davis, C., Schiller, M., & Wheeler, K. (2007). IT Auditing: Using Controls to Protect Information Assets. McGraw-Hill Osborne Media.

[4] Ernst & Young. 2009. *Global Information Security Survey*.

[5] ITGI. (2007). CobiT 4.1 – Framework, Control Objectives, Management Guidelines and Maturity Models, USA: IT Governance Institute.

[6] Min, Y. W. (2009). Understanding and Auditing IT Systems. Peking: Lulu.

[7] Panian, Z., & Spremic, M. (2007). Korporativno upravljanje i revizija informacijskih sustava. Zagreb: Zgombić & Partneri.

[8] Selig, G. J. (2008), Implementing IT Governance. Van Haren Publishing.

[9] Senft, S., & Gallegos, F. (2009). Information Technology Control and Audit (Third ed.). Boca Raton, USA: Taylor & Francis Group.

[10] Stanisic, M., & Radovanovic, D., & Lucic, D. (2010). Revizija informacionih sistema. Singidunum revija. Belgrade.