Using the Cobit 5 for E-health Governance

Melita Kozina, Ines Sekovanić
Faculty of Organization and Informatics
University of Zagreb
Pavlinska 2, 42000 Varaždin, Croatia
{melita.kozina, isekovani}@foi.hr

Abstract. *Cobit 5 provides a comprehensive framework that assists enterprises in achieving their objectives for the governance and management of enterprise information technology (IT). Furthermore, it helps enterprises create optimal value from IT based on the balance between the achieved IT benefits and the optimized risk and resource use. The implementation of e-health governance within health care is very complex project and poorly understood. The paper explores the application of this framework within the health organization in Croatia as well as its impact on e-health governance maturity and strategic alignment with health care. This study used Cobit 5 management guidelines for some of IT related activities in order to help organizations make better e-health investment decisions and strategies.*

Keywords. Cobit 5 framework, e-health governance, business-to-e-health strategic alignment, IS auditing.

1 Introduction

The purpose of the paper is to demonstrate how the principles of Cobit 5 framework (Control Objectives for Information and related Technology) can be applied in the health care. Today's information technology (IT) allows better patient health care. Providing health services is simplified by use of information technology. E-health of the future will be the backbone of the modern society.

The paper explores the application of this framework within the health organization in Croatia as well as its impact on e-health governance maturity and strategic alignment with health care. Furthermore, within this study we used the Cobit 5 management guidelines for some of IT related activities in order to help organization make better e-health investment decisions and strategies.

The research method is mainly based on the interviews with Chief Information Officer and the process owners and their documentation.

The concept of the Cobit 5 framework is described in the Chapter 2. In what way can we suggest to executive management that it use Cobit 5?

Cobit 5 offers various management tools and some of them we applied through this study [8,9]. Business-to-e-health strategic alignment refers to applying IT within health care according to the strategy of the health care organization. It is described in the Chapter 3.

IT/IS auditing within the health care organization is described in the Chapter 4. Scope of this auditing includes two representative IT processes within the IT function as well as the management guidelines related to the process goals and metrics and RACI matrix.

In conclusion, the obtained results are compared in order to represent the actual maturity level of the e-health governance within the observed health care organization.

2 Cobit 5 framework

Nowadays, there is an increasing interest considering investments in information technology and information systems. To make such investments last effectively it is necessary to set a good IT infrastructure and adapt it to the business enterprise. Using the Cobit 5 we can monitor the development and management of the information and communication systems and the design of business processes.

Enterprise governance of IT is an integral part of overall enterprise governance that ensures that IT creates value for the enterprise and broadens its strategy [5]. Cobit 5 framework includes:

a) 5 principles
b) 5 process domains
c) management guidelines for each of IT related activities (goals, metrics, practices, RACI matrix, etc.)
d) process capability model based on the ISO/IEC 15504 standard.

There are five principles of Cobit 5 framework like shown in Fig. 1. These principles are:

1. Meeting Stakeholder Needs

2. Covering the Enterprise End-to-end
3. Applying a Single Integrated Framework
4. Enabling a Holistic Approach
5. Separating Governance from Management.

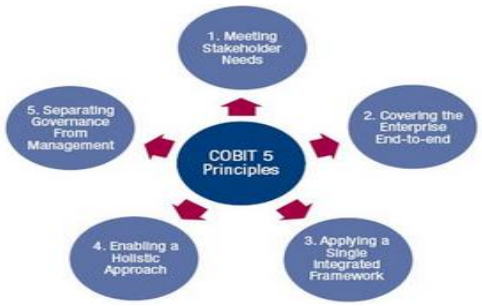

Fig. 1. Cobit 5 principles [5]

Companies exist so they could create value for their stakeholders. In order to achieve good value for their stakeholders it is necessary to have good governance and management of information and IT assets [2]. Company committees, CEOs and management need to accept IT as any other important part of the business. Cobit provides a comprehensive framework that helps businesses to achieve their goals and create value through efficient corporate governance of IT. The stakeholder needs have to be transformed into enterprise strategy. The goal of Cobit is to translate the stakeholder needs in the specific enterprise and IT objectives (shown in Fig 2) [6].

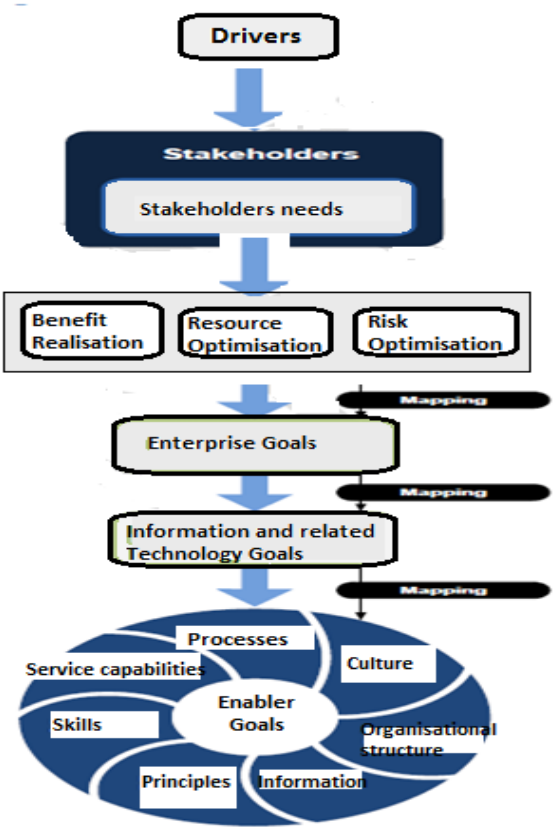

Fig. 2. Cobit 5 cascade goals overview

There are 37 processes within the Cobit 5 framework. These processes can be divided into five logical domains. Each of these processes has its own detailed controls. Domains and processes are needed so that all IT solutions can be implemented. They represent a tool for planning, implementation and use of information systems. Process domains of the Cobit 5 framework are:

a) **Governance Domain**: Evaluating, Direction, Monitorin , EDM.
b) **Management Domains:**
Align, Plan and Organize, APO
Monitor, Evaluate and Assess, MEA
Delivery, Service and Support, DSS
Build, Acquire and Implement, BAI.

In addition, Cobit 5 framework defines the Process Capability Model (Cobit 5 PAM) in order to assess the capability each of the IT process according to the 6 levels of capability (shown in Table 1).

Level	Name	Description
0	**Incomplete Process**	The process is not implemented or does not achieve his purpose (partially executed).
1	**Performed Process**	The process is implemented and it fulfills its purpose.
2	**Managed Process**	The process that executes its purpose (Level 1) and is managed (the process is planned, supervised, adjusted) and operating results are defined, controlled and maintained.
3	**Established Process**	A managed process (Level 2) is now implemented as a defined process that is capable of bringing their work performance.
4	**Predictable Process**	Defined process (Level 3) now carries out its work results within defined limits of control . The process is controlled and can be anticipated.
5	**Optimising Process**	Predictable process (Level 4) is continuously improved in order to achieve business goals of the organization , higher quality and the needs of customers / users.

Table 1. Cobit 5 Process Capability Levels

3 Business-to-e-health strategic alignment using the Cobit 5

Business-to-e-health strategic alignment refers to applying IT within health care according to the strategy of the health care organization.

E-health governance can be defined as the IT responsibility by the business and IT management within the health organization for the new organizational structures and processes that provide the business value of IT and achieve the needs of the health care stakeholders.

In this part, we used the concept of the business-to-e-health strategic alignment based on the mapping the business and IT goals of the health organization. It is based on the generic concept of the alignment between the business and IT goals defined within the Cobit 5 framework.

BSC dimension	Goals	Metrics
Finance	Being aligned with prices of HZZO	Price of health services
	To stay within the allowed limits	Monthly Report of spent funds
	Annual planning	The percentage of funds spent
Customers	Increasing the number of patients	Number of patients
	Reducing waiting lists	The number of patients on the waiting list
	Quality of patient treatment	Quality indicators of treatment
Internal business processes	Improving the service process	Number of days waiting for service
	The increase in revenues as a good way of invoicing services	The amount of revenue from invoicing
	Reduction of repeated service	Number of repeated service
Learning and growth	Employee training	The cost of employee training
	Training to work on new apparatuses	The percentage of accuracy in the execution of the new apparatuses

Table 2. Business BSC strategy map of the health organization

The stakeholder needs can be associated with the governance objective of the health organization. Governance goals are related to obtaining benefits, risk management and cost optimisation. Governance objectives of the hospital are mapped into a set of generic objectives that are made using the BSC (Balanced Scorecard) strategy map through the four perspectives: *finance, customers, internal business processes and learning and growth* [7]. Table 2 shows business BSC strategy map of the health organization.

Hospital objectives require a certain number of IT outputs. These IT outputs are shown as IT goals. Table 3 shows the results of the mapping between IT goals and the health care goals of the hospital.

BSC dimension	IT goals
Business contribution of IT	Improved invoicing system services
	Increased employee productivity
	A better flow of patients through the hospital
	Reducing the cost of treatment
Customers	Update application e - ordering
	Regularly updated information on a patient in the hospital information system
	Keep the complaints of patients within the PIS application
Internal Processes	Reduce the waiting time for service by computerizationing the process of waiting patients on the service
	Improve the billing services process by regular updating and improving business application PIS
	Avoid redundancy data by maintaining the BIS system (central information system of the hospital)
Learning and Growth	Enable employees to work with new ERP system
	Train new employees to work with applications

Table 3. IT BSC strategy map as result of the business to e-health strategic alignment

The business contribution dimension evaluates the IT performance from the viewpoint of top management and the stakeholders [2]. *The business value of IT projects* can be measured through the financial measures such as ROI, Cost/Benefit Analysis, through the measures focused on service improvements related to health care, as well as

through those measures that are based on enabling the achievement of corporate health strategy. **In this business case the business contribution of IT** is especially related to the improved invoicing system services, increased employee productivity, a better flow of patients through the hospital, reducing the cost of treatment.

IT BSC is a measurement and management system very suitable for supporting the IT Governance process and the IT/Business Alignment process [11]. The essence of IT Governance is to ensure the mechanism which will link business and information systems (strategy alignment), initiate continual improvement of IT in order to extend the organization's strategy and objectives [1].

4 IT/IS auditing within the health care organization using the Cobit 5

An audit of information systems is the process of the evaluation of the established control mechanisms and procedures as well as the assessment of compliance with "good practices", standards and methods; identification the weaknesses and risks.

For the purpose of this study we selected two processes of IT function within the health organization and applied some of the management guidelines according to the Cobit 5 in order to identify the weaknesses and risk and suggest the adeqaute improvements. The process *Ensure risk optimisation* is the governance process (EDM process domain) from the Cobit 5 Process Reference Model. The process *Manage quality* is the management process (APO process domain) .

Process goals	Related metrics
(1)The thresholds of risk are defined and key IT risks are known	The number of potential IT risks that are identified and controlled The level of evaluation of risk factors The level of relations between IT risks and enterprise risk
(2) The company manages critical IT risks effectively and efficiently	The percentage of company projects that consider IT risks Percentage of IT risks plans that are carried out on time The percentage of critical risks wich were effectively mitigated
(3) IT risks of the company do not exceed the tolerance for risk and the impact of IT risk to the value of the company is identified and controlled	The percentage of IT risks that exceed the tolerance for risk Level of unexpected impact on the company

Table 4. Process goals and related metrics - *Ensure risk optimisation* (Cobit 5 framework)

For audit of these processes, we applied two Cobit techniques. The first technique is related to **the process goals and their measurement** by means of the relevant metrics. Other technique is related to **the RACI matrix** for the specific process.

The process *Ensure risk optimisation* should enable that risks and risk tolerance are understood and that the risks associated with the creation of enterprise value by using IT are identified and managed. The purpose of the process is to ensure that the impact of IT risk on the value of the company is identified and that the errors are reduced .

A**ccording to the Cobit 5 framework**, this process has three process goals and related metrics (shown in Table 4) [5].

We explored the process goals and metrics for the risk management within the hospital and got the following results (shown in Table 5).

Process goals	Metrics
(1)Reduce the number of interruptions or difficulties in business functioning	The monthly number of business interruptions due to the decline of the information system
(2)Reduce the risk of attacks on information system property	Number of irruptions in the information system
(3) Secure sensitive information from theft	Number of stealing sensitive data
(4)Reduce risk due to inadequate protection of cryptographic keys	The level of protection of cryptographic keys
(5)Prevent illegal downloading and use of software	Number of illegally downloaded software
(6)Better protection of information system passwords	Level of password protection in information system
(7)Monthly testing of errors and viruses in the information system	Number of found errors and viruses

Table 5. Process goals and related metrics - *Ensure risk optimisation* in the hospital

Based on the auditing of the *Ensure risk optimisation* within the health care organization, a few deficiencies were found. The first lack is related to the number of crashs of the information system. Namely, that it is a newly introduced system, the number of falls and the monthly business interruptions due to system crashes are quite common.

All departments and patients in the hospital depend on the work of the information system.

It is recommended to test the system and use troubleshooting on the system during the late afternoon hours, when there are less patients in the hospital , and not, as now, in the early morning hours.

Furthermore, the lack is found associated with the weak password protection. Although this is highly sensitive data, password management in the hospital is bad. The security of the passwords is on a low level and includes mostly four random characters. Password changes on a monthly basis don't exist, which means that the information system security is endangered due to inadequate management of the passwords.

Monthly testing of errors and viruses is not carried out although there is NOD program to prevent the viruses, most of the medical and non-medical staff are not trained to work with him, leading to a large number of viruses and errors. Program running and cleaning computer from viruses is carried out once a year which is too little .

Better information system security would improve the quality of treatment of the patient and there would be less interruptions in the operation of the system .

Based on the our assessments, we can conclude that the process goals relative to the Cobit 5 standard are partially implemented - up to 15 % . The hospital should improve the IT risk management in order to avoid disruption of the system. It is necessary to control the impact of IT risk to the onset of security holes in the system.

Another technique that we used is the RACI matrix (shown in Table 6). It consists of the acronyms which mean [5]:

-**Responsible** (person who has operational responsibility for the performance of work);

-**Accountable** (a person who is personally responsible and gives final approval);

-**Consulted** (the person giving support in the form of reviews, tips and explanations);

-**Informed** (the person who reports about the events).

RACI matrix of the process *Ensure risk optimisation* within the hospital practice has several disadvantages. The hospital has its own head of information security and he is, along with the head of IT, in charge of the risk management. The role of the hospital board in the risk management is minor and it should be, according to the Cobit, increased. However, there is a problem in accountablity, because too many people are accountable for risk optimisation, leading to frequent confusion. Due to the large number of informed people there is the question of whether everyone should be informed?

Practice	Board	Hospital director	CFO	Head of Accounting	CIO	Lead programmer	COO	IT security director
Evaulate risk management	I	A	C	C	R	C	C	R
Direct risk management	I	A	I	I	A	C	C	R
Monitor IT risk management	I	A	I	I	A	C	C	R

Table 6. RACI matrix for *Ensure risk optimisation* in the hospital

Further, the next process, at the management level, which we analyzed, is the process APO11 – Manage Quality. This process serves to define requirements for quality in all processes, procedures and related outcomes of the hospital including the control, supervision and the use of standards and practices in the continuous improvement. It serves to ensure the consistent delivery of solutions and services that meet the quality requirements of the hospital and the needs of stakeholders .

Process goals	Related metrics
(1)Stakeholders are satisfied with the quality solutions and service	Percentage of stakeholders satisfied with IT quality Number of services with a formal plan of quality management The average rating of the stakeholders satisfaction with solutions and service
(2)Results of the project and services delivery are predictable	The percentage of solutions and services delivered with the official certificate The number of detected defects before production The percentage of inspected projects that meet the desired quality goals
(3) Quality requirements are implemented in all processes	Number of processes with defined requirements for quality Number of processes with formal report on the quality Number of SLAs that include eligibility criteria for quality

Table 7. Process goals and related metrics for *Manage quality* (Cobit 5 framework)

The process - *Manage quality* according to the Cobit 5 framework has three process goals and related metrics (shown in Table 7) [5]. Process goals and related metrics for *Manage quality* were explored within the hospital practice (shown in Table 8).

Process Goals	Metrics
(1)Involve IT service in "Quality management plan of the hospital“	The percentage of informatics involvement in "Quality management plan of the hospital "
(2)Collect proposals for the development and improvement of the Hospital Information System	Number of proposals for Hospital Information System improvement
(3)Implementation of nursing documentation in the information system	Percentage of completed implementation of nursing documentation in the information system
(4)Document all hospital software	The amount of documented hospital software
(5)Maintain hospital applications	Number of well-maintained hospital application

Table 8. Process goals and related metrics for *Manage quality* in the hospital

The hospital has a quality management plan. However, **the role of information technology and IT department in the plan is minor.** It is necessary to maintain the IT quality at the appropriate level to enable better support for other processes of the hospital .

Another of the deficiencies found is linked to the collection of proposals for improvement and development of the hospital information system. Suggestions are always welcome, and they show that the IT department works as a team to improve the system. However, in practice interest of IT staff for presenting such proposals was not found. Proposals that were present were not implemented in reality because of weak mutual communication and employee resistance to it. It is necessary to work on teamwork to enable quality business.

The lack was found in documenting the software. Documenting helps with better software maintenance. There has not been found satisfactory software documentation in the hospital. The documentation is done in an unprotected Excel table that is not stored anywhere permanently**. Based on the our assessments, we can conclude that the process goals relative to the Cobit 5 standard are also partially implemented - up to 15 % .**

The results of the analysis related to the organizational structures and their responsibilities through the practices of the *Manage Quality* are shown in the Table 9.

Practice	Board	Hospital director	CFO	Head of Accounting	CIO	Lead Programmer	COO	Quality management team
Establish a quality management system	I	C	I	I	A	C	I	A
Define and manage quality standards, practices and procedures	I	C	I	I	A	C	I	A
Focus quality management on customers	I	C	I	I	R	C	I	A
Perform quality monitoring, control and reviews	I	I	I	I	R	C	I	A
Integrate quality management into solutions for development and service delivery	I	I	I	I	R	C	I	A
Ensure continuous improvemnt	I	C	I	I	R	C	I	A

Table 9. RACI matrix for *Manage quality* in the hospital

As can be seen from the RACI matrix, the main responsibility for the quality management has the quality management team at the hospital as well as the head of IT (CIO**). Their roles often lead to the confusion within the decision-making.**

5 Conclusion

The goal of the paper was to analyze how the application of the Cobit 5 framework within the health organization can be useful for the e-health management in order to improve the maturity of e-health governance and strategic alignment with health care.

Cobit 5 framework provides different tools for increasing the maturity of enterprise governance of

IT. Some of them we applied for this study in order to compare the actual maturity level of e-health governance within the observed organization with the target level of the maturity.

The business-to-e-health strategic alignment was conducted within the health care organization using the Cobit 5 management guidelines and the Balanced Scorecard strategy maps. It is very important measurement and management mechanism to support the e-health governance. Using this mechanism, we could analyse how the hospital and the board evaluate the business value of IT and how much IT is involved into the health care services.

The purpose of the IT/IS auditing within the health care was to identify existing weaknesses and risks and suggest the needed improvements. We used also Cobit 5 management guidelines for the IT processes (process goals and metrics and RACI matrix). We selected the governance process from Cobit 5 process reference model (*Ensure Risk Optimisation*) and the management process (*Manage Quality*). The obtained results showed that the capability of these processes is very low.

Through the methods and tools that we used, we can make the conclusion that IT function has good basis for the improvements. The improvement projects within the hospital are primarly focused on the implementation of the information security management system as well as on the implementation quality management system within IT function. Furthermore, the hospital should improve the alignment between business and IT objectives, include more IT solutions/ IT services into the business processes, to improve the central hospital IS as well as the responsibilities of business and IT managers in the field of IT investments.

References

[1] De Haes, S.,Van Grembergen,W.: *IT Governance Structures, Processes and Relational Mechanisms: Achieving IT/Business Alignment in a Major Belgian Financial Group*, Proceedings of the 38th Hawaii International Confernce on System Sciences, 2005.

[2] Gregor, S, Fernandez.: *Achieving value from ICT: key management strategies*, Department of Communications Information Technology and theArts,http://cs.anu.edu.au/courses/COMP3120/public_docs/Achieving_Value_from_ICT_-_Key_Management_Strategies.pdf, Accessed: 2015-05-04.

[3] Guldentops, E.:*Value Management Principles*, ISACA, 2007.

[4] Harmer, G.: Governance of Enterprise IT based on Cobit 5, ITGI, UK, 2013.

[5] ISACA Cobit 5: Process Reference Guide, ISACA, 2011.

[6] ISACA CGEIT Review Manual 2015, 2015.

[7] Kapur, R.:*Use of the Balanced Scorecard for IT Risk Management*, ISACA, 2010.

[8] Lambeth, J.:*Using Cobit as a Tool to Lead Enterprise IT Organizations*, ISACA, 2007.

[9] Selig, Gad J.: *Implementing Effective IT Governance and IT Management*, Van Haren Publishing, (Second Edition) 2015.

[10] Thorp J.:*Enterprise Value: Governance of IT investments*,The Val IT Framework",ITGI, 2008.

[11]Van Grembergen,W., De Haes, S.: *IT Governance ad its mechanisms*, Information Systems Control Journal, vol.1., 2004.