IT Risk Management in the enterprise using CobiT 5

Melita Kozina
University of Zagreb
Faculty of Organization and Informatics
Pavlinska 2, 42 000 Varaždin, Croatia
mkozina@foi.unizg.hr

Abstract. *The purpose of the paper is to demonstrate how to manage IT risks in an enterprise using an IT Governance framework such as the CobiT 5 and Balanced Scorecard (BSC) method integrated within this framework. The BSC method will help business and IT management build business strategy based on the stakeholder needs as well as generate relevant IT strategy. The CobiT 5 framework offers generic models for BSC/IT BSC strategic maps and links them to IT processes. A company of any size and industry can use such models and adapt them to its business practice. Mapped IT processes and aligned with business and IT goals are the basis for identifying possible IT risks as well as the likelihood of their occurrence and consequences for business. These tools were used within a specific institution for the purpose of this research. The research method is mainly based on the interviews with the business executives, process owners, Chief Information Officer, IT managers and the security manager.*

Keywords. IT Risk Management; IT Governance; BSC/IT BSC strategy; CobiT 5 framework

1 Introduction

This paper aims to present the contribution of the CobiT 5 framework and its tools in IT risk assessment and to facilitate managers' effective IT risk management (Lambeth, 2007). The importance of the IT Risk Management process is described in Chapter 2. There are different methods and tools for IT Risk Management. The applied methodology in the paper comprises CobiT 5 principle 1 relating to alignment of the business strategy and the IT strategy through the Balanced Scorecard (BSC) method integrated within CobiT 5.

Furthermore, IT processes are mapped with relevant IT objectives according to the CobiT 5 guidelines. IT processes mapped with business and IT goals are a key basis for identifying possible IT risks as well as the likelihood of their occurrence and consequences for business. The methodology is described in Chapter 3. The research results are described in Chapter 4.

The research was conducted in one of the leading banks in Croatian business practice using the above tools.

The research method is based on the interviews with the business executives, process owners, Chief Information Officer, IT managers and the security manager. Data collection is based on the respondents' statements and their documentation.

The scientific contribution of the paper is the conducted research and analysis of the results related to the IT risk management using the IT governance methodology. The applied methodology can assist business and IT management in mapping business and IT goals and further mapping IT goals and IT processes. Each mapped IT process which primarily supports IT goals (IT strategy) can be a potential source of IT risk that threatens the business. The applied methodology helps management to identify potential risks and assess the level of risk acceptance for business when mapping business and IT objectives.

2 IT Risk Management

IT Risk Management is a systematic analytical process by which an organization detects, identifies, reduces and monitors potential risks and losses to which it is exposed. IT risks are risks that arise from the intensive use of business information systems and technology as an important support to the development and improvement of business processes (Spremić,2005).

Risk can be defined as the likelihood that an appropriate source of threat in certain circumstances will exploit the vulnerability (weakness) of the system, which, consequently, may cause some damage to the assets of the organization.

Why is the corporate IT risk management process important? The following are the main reasons (Spremić,2005):

- Risk of unprofitable investments in informatics;

- Risk of unsuccessful implementation of IT projects;
- Risk of business interruption or difficulty;
- Risk of attack on information system assets;
- Risk of theft of sensitive data;
- Risk of growing complexity of information systems;
- Technological risks.

The general concept of the IT risk management process is shown in Figure 1 (part of the risk management framework taken from the ISO 31000 standard). The IT risk management plan is a systematic process that includes the following steps:

- identification of all IT risks;
- determining the level of IT risks by assessing their 'severity' (impact on business and assets) and frequency of occurrence;
- determining countermeasures to identified risks by setting up IT controls;
- assignment of responsibilities and implementation and documentation of IT controls;
- constant supervision and revision of the IT risk management plan.

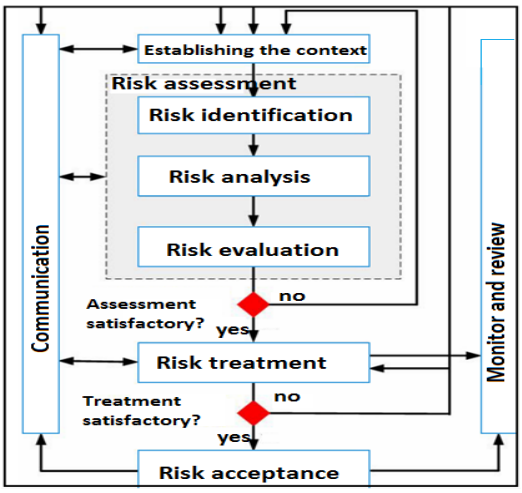

Figure 1. The Risk Management process (ISO 31000:2018)

Risk is a combination of the likelihood of a particular threat and its consequences for business. Determining the likelihood of occurrence and the level of consequences for the identified threat is given by the risk value table, shown in Figure 2. The table was used in the research (Spremić,2005).

		likelihood of occurrence		
		Small (1)	Medium (2)	Large (3)
consequences	Small (1)	1	2	3
	Medium (2)	2	4	6
	Large (3)	3	6	9
	Very large (4)	4	8	12

Figure 2. Risk value table

Acceptable level of risk - risk that does not threaten the development of important business functions and processes.

3 IT Governance CobiT 5 framework

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 (Selig, 2015). CobiT 5 framework offers different tools and supports IT governance (Lambeth, 2007). It includes: a) 5 principles b) 5 process domains c) management guidelines for each of IT related activities (goals, metrics, practices, RACI matrix) d) process capability model based on the ISO/IEC 15504 standard. CobiT 5 principle 1 was used in this research (ISACA CobiT 5, 2012). Some of researchers develop initial view of relationships between business goals, IT goals and IT processes (Van Grembergen et al., 2005). The stakeholder needs should be transformed into enterprise strategy and IT strategy (shown in Figure 2).

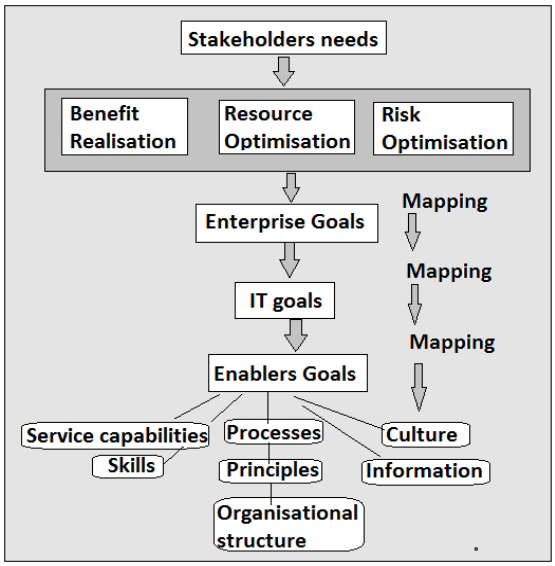

Figure 2. CobiT 5 principle 1

CobiT 5 and Balanced Scorecard (BSC) method are the main IT governance mechanisms (Van

Grembergen & De Haes, 2004). These mechanisms will help business and IT management build business strategy based on the stakeholder needs as well as generate relevant IT strategy. The CobiT 5 framework offers generic models for BSC/IT BSC strategic maps (***17 business goals and 17 IT goals)*** and links them to IT processes. A company of any size and industry can use such models and adapt them to its business practice.

Mapped IT processes, business and IT goals are the basis for identifying possible IT risks as well as the likelihood of their occurrence and consequences for business. Balanced scorecards are one of a number of quantitative tools available to support risk planning (Olson&Wu,2020). These tools are used within a specific financial institution for the purpose of this research. IT governance methodology for the IT risk management is shown in Figure 3. Steps 1 to 7 were applied for this study.

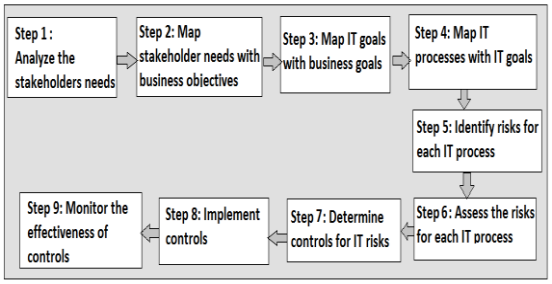

Figure 3. IT governance methodology for the IT risk management (source: Author)

4 Analysis of research results

This chapter describes and analyzes the results of research using IT governance methodology that comprises CobiT 5 framework and BSC / IT BSC methods. The methodology was applied for the purpose of risk assessment according to the IT risk management process taken from the ISO 31000 standard (ISO 31000, 2018).

The CobiT 5 framework defines a generic map of 17 strategic business goals that each company can adjust to its practice. These goals are arranged according to the perspectives of the BSC method such as finance, customers, processes, and learning and growth. The following are the BCS goals:

BSC Financial:

1. Stakeholder value from business investment
2. Portfolio of competitive products/services
3. Managed business risk
4. Compliance with external laws and regulations
5. Financial transparency

BSC Customer:

6. Customer oriented service culture
7. Business service continuity and availability
8. Agile responses to a changing business environment
9. Information based strategic decision making
10. Optimisation of service delivery costs

BSC Internal:

11. Optimisation of business process functionality
12. Optimisation of business process costs
13. Managed business change programmes
14. Operational and staff productivity
15. Compliance with internal policies

BSC Learning and Growth:

16. Skilled and motivated people
17. Product and business innovation culture.

The CobiT 5 framework defines a generic map of 17 IT strategic goals that each company can adapt to its IT function. These goals are arranged according to the perspectives of the IT BSC method, such as finance (business contribution), customer / users, internal / IT processes, and learning and growth. The following are IT BSC goals:

IT BSC Financial/Business Contribution:

1. Alignment of IT and business strategy
2. IT Compliance and support for business compliance
3. Commitment of executive management for making IT-related decisions
4. Managed IT-related business risk
5. Realised Benefits from IT-enabled investments and service portfolio
6. Transparency of IT costs, benefits and risk

IT BSC Customer/User:

7. Delivery of IT services in line with business requirements
8. Adeqaute use of applications, information and technology solutions

IT BSC Internal/IT processes:

9. IT agility
10. Security of information, processing infrastructure and applications
11. Optimisation of IT assets, resources and capabilities
12. Enablement and support of business processes by integrating applications and technology into business processes
13. Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards
14. Availability of reliable and useful information for decision-making
15. IT compliance with internal policies

IT BSC Learning and Growth:

16. Competent and motivated business and IT personnel
17. Knowledge, expertise, and initiatives for business innovation.

4.1 Interview and research protocol

The applied methodology is shown in Figure 3 starting from step 1 to step 7. The interview and research protocol is described below.

According to steps 1 and 2 it is necessary to analyze the needs of stakeholders with regard to the realization of IT benefits including the optimization of risks and costs within the bank. After that, it is necessary to map the needs of stakeholders and business goals of the bank. For this part of the research, from the Cobit 5 framework, BSC business goals 1, 3, 6, 7, 10, 11, 13, 16 and 17 were selected (shown in Table 1).

For BSC financial aspect: an interview was conducted with the Chief Executive Officer (CEO), Chief Information Officer (CIO) and business risk manager within the bank regarding the requirements for computerization of bank operations and achieving business value of IT (shown in Table 1). The research questions were designed for this purpose: *How can you best exploit new technology for new strategic opportunities and revenue growth? How do you get value from the use of IT? Did you adress all IT related risks?*

For BSC customer aspect: an interview was conducted with the CEO and CIO regarding the requirements for achieving the quality of IT services, continuity of IT services and customer satisfaction (shown in Table 1). The research question was designed for this purpose: *Are end users satisfied with the quality and warranty of IT services?*

For BSC internal aspect: an interview was conducted with the business executive manager, project manager and CIO regarding the requirements for modernization of sales channels, competitiveness of banking operations and development of new products (shown in Table 1). The research question was designed for this purpose: *How successful are IT projects?*

For BSC learning and growth aspect: an interview was conducted with the human resources manager regarding the requirements for staff education and promoting an innovation culture (shown in Table 1). The research question was designed for this purpose: *How do you develop skills for employees and promote an innovation culture?*

Stakeholder needs are mapped with CobiT 5 business goals that are aligned and adapted to the business practices and needs of the bank.

Table 1: Strategic stakeholder analysis and mapping IT goals with business goals (source: Author)

	Mapping stakeholder needs with the business goals						Mapping IT goals with the business goals			
	Stakeholder needs						Enterprise goals			
BSC aspect	Enterprise goals	IT benefits	IT Risk Optimisation	IT Resource Optimisation	IT BSC aspect	IT goals	Financial	Customer	Internal	Learning and Growth
Financial	1. Stakeholder value of business investments	Higher ROI, Revenue Growth			Financial/ Business contribution	1. Alignment of IT and business strategy	1. Stakeholder value of business investments	6. Customer-oriented service culture	11. Optimisation of business process functionality 13. Managed business change programmes	
	3. Managed business risks		IT related risk optimisation			4. Managed of IT related business risks	3. Managed business risks	7. Business service continuity		
Customer	6. Customer-oriented service culture	Customer satisfaction				5. Realised benefits from IT investments	1. Stakeholder value of business investments			
	7. Business service continuity	IT service quality	Warranty of IT services		Users of IT services	7. Delivery of IT services in line with business requirements	1. Stakeholder value of business investments	6. Customer-oriented service culture	11. Optimisation of business process functionality	
	10. Optimisation of service delivery costs			IT related costs optimisation		8. Adequate use of application		10. Optimisation of service delivery costs	11. Optimisation of business process functionality	
Internal	11. Optimisation of business process functionality	Competiveness of the bank's business processes			Internal IT processes	10. Security of information		7. Business service continuity		
	13. Managed business change programmes	New product development; modernization of sales channels	IT related risk optimisation	IT related costs optimisation		12. Support of business processes by integrating application and technology into business processes			11. Optimisation of business process functionality	
Learning and growth	16. Skilled and motivated people			Educated bank staff	Future orientation	16. Competent and motivated business and IT staff				16. Skilled and motivated people
	17. Product and business innovation culture	Culture of business innovation				17. Knowledge and initiatives for innovation				17. Product and business innovation culture

The following are a few examples. Stakeholder needs for higher revenue growth (IT benefit) are mapped with the business goal 1 - *Stakeholder value of business investments*.

Furthermore, the stakeholder needs to ensure the warranty of IT services (Risk optimisation) and the quality of IT services (IT benefits) are mapped with the business goal 7 - *Business service continuity and availability*. The stakeholder needs for the competitiveness of the bank's business processes (IT benefits) are mapped with the business goal 11 - *Optimization of business process functionality*. The stakeholder needs to promote an innovation culture within the bank (IT benefits) are mapped with the business goal 17 – *Product and business innovation culture.*

Furthermore, according to the protocol and step 3 of the applied methodology, it is necessary to map IT goals and business goals. For this purpose, an interview with the CIO was conducted. IT BSC goals 1, 4, 5, 7, 8, 10, 12, 16 and 17 were selected from the Cobit 5 framework. The main research question was: *Which IT goals can be mapped with the bank's business goals according to the Cobit 5 guidelines*?

Table 1 shows the mapping results of IT BSC goals (1, 4, 5, 7, 8, 10, 12, 16 and 17) with the BSC business goals (1, 3, 6, 7, 10, 11, 13, 16 and 17). The following are a few examples.

IT BSC goal 1 - *Alignment of IT and business strategy* primarily supports the following business goals: 1 - *Stakeholder value of business investments*; 6- *Customer-oriented service culture*; 11 - *Optimization of business process functionality* and business goal 13 - *Managed business change programs*.

Furthermore, the IT BSC goal 7 -*Delivery of IT services in line with the business requirements* primarily supports the following business goals: 1 - *Stakeholder value of business investments*; 6 - *Customer-oriented service culture*; 11-*Optimization of business process functionality*.

IT BSC goal 8 - *Adeqaute use of applications, information and technology solutions* primarily supports the following business goals: 10 - *Optimization of service delivery costs* and business goal 11 - *Optimization of business process functionality* (shown in Table 1), etc.

According to the protocol and step 4 of the applied methodology, it is necessary to map IT processes and IT goals (shown in Table 2). For this purpose, an interview with the CIO was conducted within the bank. The main research question was: *Which IT processes can be mapped with the IT goals according to the Cobit 5 guidelines*?

The CobiT 5 framework offers a process reference model that includes 37 processes across 5 domains: EDM (Evaluate, Direct and Monitor); APO (Align, Plan and Organize); BAI (Build, Aquire and Implement); DSS (Deliver, Service and Support); MEA (Monitor, Evaluate and Assess).

The selected IT process can have a primary impact on more IT goals (shown in Table 2). The following are a few examples.

IT Process APO02 – *Manage strategy* has primary impact on the IT goals 1, 7 and 12 (shown in Table 2). IT Process APO07 – *Manage human resources* has primary impact on the IT goals 1, 16 and 17. IT Process APO09 – *Manage service agreement* has primary impact on the IT goal 7. IT Process APO11 – *Manage quality* has primary impact on the IT goals 5 and 8 (shown in Table 2), etc.

Last step in the interview and research protocol is described below. According to the applied IT governance methodology for the IT risk management, shown in Figure 3, steps 5, 6 and 7 are following.

The results related to the identification of possible IT risks for each IT process are shown in Table 2.

Research questions for IT managers (strategy, risks, quality, security, services and resources) included the following items:

- What threats can be identified for each process?
- What is the likelihood of the threat occurring?
- What is the level of consequence for the identified threat?
- What is the level of risk / treatment?

Determining the likelihood of occurrence and the level of consequences for the identified threat is given by the risk value table, shown in Figure 2.

The likelihood of the threat occurring, the level of business impact and the level of risk according to the risk value table was determined for one of the identified threats per individual IT process (bold font) (shown in Table 2). In accordance with the assessed level of risk, a proposal for corrective action to reduce the risk was defined (shown in Table 2).

Table 2: Mapping IT processes with IT goals/ IT Risk Management for mapped IT processes (source: Author)

Mapping IT processes with IT goals			Research questions/IT risk assessment			
Cobit 5 IT process	**Primary impact of the IT process on the following IT goals:**	**Purpose of Cobit 5 IT process**	**What threats can be identified? Answers:**	**What is the likelihood of the threat occuring? Answers:**	**What is the level of the consequence for the identified threat? Answers:**	**Assessed level of IT risk/proposed corrective action**
APO02 Manage Strategy	1. Alignment of IT and business strategy 7. Delivery of IT services in line with business requirements 12. Support of business processes by integrating application and technology into business processes	Assess the existing IT environment and define the future strategic IT plans aligned with the business goals.	**1) the strategic IT plan is not complete** 2) business and IT goals are not aligned 3) poor integration of IT and business processes 4) activities related to communicate the IT strategy are not defined	**(1) small**	**(4) very large**	**(4) medium** **It is necessary to complete a strategic IT plan**
APO07 Manage Human Resources	1. Alignment of IT and business strategy 16. Competent and motivated business and IT staff 17. Knowledge and initiatives for innovation	Optimise the human resource capabilites to meet enterprise goals.	1) the required IT skills and competencies are not defined 2) **formal staff training is not defined** 3) there is no planning and monitoring of the usage of IT and business human resources 4) poorly managing contract staff 5) **there is no continuous verification of IT competencies**	**(3) large**	**(2) medium**	**(6) medium** **Formal staff training should be defined as well as the verification of IT competencies**
APO09 Manage Service Agreements	7. Delivery of IT services in line with business requirements	Ensure that IT services meet current and future business needs.	1) business requirements and the way IT services support business processes are not analyzed 2) poorly defined SLA contracts **3) the realization of agreed service levels is not monitored**	**(2) medium**	**(3) large**	**(6) medium** **The realization of agreed service levels should be monitored**
APO11 Manage Quality	5. Realised benefits from IT investments 8. Adequate use of application	Provide delivery of solutions and services aligned to quality requirements of the enterprise and satisfy stakeholders needs.	1) there is no defined QMS plans 2) quality standards are not defined 3) QMS does not focus on customers **4) poor integration of QMS into solution development and service delivery**	**(2) medium**	**(3) large**	**(6) medium** **Integration of QMS principles into solution development and service delivery should be complete**
APO12 Manage Risk	4. Managed of IT related business risks 10. Security of information	Integrate IT risk management in the overall business and business risk management. Balance the benefits of IT investments along with costs and IT risks.	**1) An IT risk management framework is not defined.**	**(2) medium**	**(4) very large**	**(8) large** **An IT risk management framework should be defined**
BAI01 Manage Programmes and Projects	1. Alignment of IT and business strategy 4. Managed of IT related business risks	Managing all programmes and projects ensuring the value and quality of project deliverables.	1) The programmes and projects plan is not developed 2) The quality of programmes and projects is not managed 3) **The risks of programmes and projects are not managed** 4) Projects are poorly implemented 5) Projects performance is not monitored	**(2) medium**	**(4) very large**	**(8) large** **The risks of programmes and projects should be managed**
BAI06 Manage Changes	4. Managed of IT related business risks 7. Delivery of IT services in line with business requirements	Manage all changes relating to business processes, applications and infastructure.	1) There is no impact assessment as well as definition of priorities and categories of change **2) There is no emergency change management prcedure** 3) The efficiency of implemented change is not monitored	**(1) small**	**(3) large**	**(3) small** **The emergency change management procedure should be defined**
DSS04 Manage Service Requests and Incidents	4. Managed of IT related business risks	Ensure timely and effective response to user request and resolution of all types of incidents.	1) There are no records, classification and prioritization of requests and incidents **2) There is no defined procedure for resolving incidents**	**(2) medium**	**(2) medium**	**(4) medium** **The procedure for resolving incidents should be defined**
DSS05 Manage Problems	4. Managed of IT related business risks	Identify and classify problems and their root causes and ensure resolution to prevent recurring incidents.	1) There is no procedure for identifying and classifying problems. **2) There are no procedures for solving problems**	**(2) medium**	**(2) medium**	**(4) medium** **The procedure for resolving problems should be defined**
DSS07 Manage Information Security	4. Managed of IT related business risks 10. Security of information	Minimise the business impact of information security vulnerabilities and incidents.	**1) There are no procedures for managing information security**	**(2) medium**	**(2) medium**	**(4) medium** **The procedure for managing inf.security should be defined**

For example, for the identified threat "*there is no strategic plan*", the likelihood of occurrence is "1.small", business impact is "4.very large", the level of risk is "4. Medium". The corrective action is: *It is necessary to develop a strategic plan for IT*.

Given the levels of risk, risks greater than 6 are critical for the institution. There are two critical risks in this study. They relate to the APO12 Manage Risk and BAI01 Manage Programs and Projects processes.

According to the answers of the respondents, it is necessary to define the framework for IT risk management within the bank as soon as possible, with special emphasis on programs and projects. Other risks are generally acceptable and do not have a dramatic impact on the bank's operations, but these risks should be controlled. In addition to initiated controls, critical risks can be transferred to a third party or should be avoided.

5 Conclusion

The applied IT governance methodology for IT risk management, which includes the CobiT 5 framework and the BSC / IT BSC methods, is effective for several reasons. One of them is a way to map the stakeholder needs with the company's strategic goals and define the business strategy. The second reason is a way to decompose business goals into technological goals and define the IT strategy.

CobiT 5 framework specifies 17 generic business goals through BSC perspectives such as finance, customers, processes, and learning and growth (Gold,2003). CobiT 5 also specifies 17 generic IT goals through IT BSC perspectives such as finance / business contribution, customers / users of IT services, IT processes, and learning and growth. Each company can adapt these goals to its practice and needs.

Furthermore, the methodology supports mapping of IT goals and IT processes. All described mappings were conducted within the bank according to the CobiT 5 guidelines and the answers of the respondents.

Based on the mapped value chain, IT goals or IT processes can be potential sources of IT risks that can threaten a company's business. The paper identifies possible risks using the described methodology (steps 1 to 7). Proposals for corrective measures to reduce risk are also defined for each assessed level of risk.

It is known that there are many methods in the literature for IT risk assessment. The purpose of this study is to support IT risk assessment using CobiT 5.

The applied methodology, based on a holistic approach, combines leading strategy management practices (Balanced Scorecard), CobiT 5 framework and IT risk management framework (mostly COSO framework and ISO 31000 standard). In this way, the applied methodology allows companies to upgrade their existing approaches to an integrated methodology (Smart &Creelman, 2013).

The following is a short section for discussion. The scientific contribution of the paper is the research and analysis of results related to IT risk management using IT governance methodology. Based on the research results in the paper, any company can adapt the elements of the applied methodology to its own practice and gradually develop an integrated methodology. Furthermore, the applied methodology in the paper was successful for one company. However, the goal of future research should focus on evaluating the described methodology in linking business goals, IT goals and IT processes as well as in identifying possible IT risks for more companies.

References

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

Gold,R. S. (2003). "Building the IT Organization Balanced Scorecard." Information Systems Control Journal 5: 46-48.

ISACA. CobiT 5 (2012): *A Business Framework for the Governance and Management of Enterprise*

ISO 31000 (2018): *Risk Management . Guidelines*

Lambeth, J. (2007): *Using Cobit as a Tool to Lead Enterprise IT Organizations*, ISACA.

Olson, D.L., Wu, D.(2020): *Balanced Scorecards to Measure Enterprise Risk* Performance. Retrieved from https://link.springer.com/chapter/10.1007/978-3-662-60608-7_10

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

Smart, A.,Creelman,J.(2013): *RBPM: Integrating Risk Frameworks and Standards with the Balanced Scorecard. Retrieved from: https://link.springer.com/chapter/10.1057/9781137367303_3.*

Spremić, M. (2005.): *Managing IT risks by implementing information system audit function,* Proceedings of the 3rd International Workshop in Wireless Security Technologies, Westminster University, London.

Uhl, A. and Gollenia, L.A. (2012). *A Handbook of Business Transformation Management Methodology*. Gower Publishing, USA.

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

Van Grembergen, W., De Haes, S., Moons, J. (2005). "Linking Business Goals to IT Goals and COBIT Processes." Information Systems Control Journal 4: 18-22.