Decision making in ITSM processes risk assessment

V Grekul*, N Korovkina, K Korneva

National Research University Higher School of Economics, 20 Myasnitskaya Ulitsa, Moscow, 101000, Russia

**Corresponding author's e-mail: grekoul@hse.ru*

Received 1 October 2015, www.cmnt.lv

Abstract

This article is dedicated to enterprise risk management, specifically the problem of subjectivity of decisions made on different phases of risk management process, risk assessment in particular. Quality of decisions strongly affects the effectiveness of risk management process as a whole; at the same time, standards regulating risk management do not provide any instruments to support the decision-making process.

The main objective of this study is to decrease the subjectivity of decisions made during the risk management process by integrating decision theory tools into the risk assessment phase. As a result, an approach to risk assessment using Analytical Hierarchy Process is introduced; the approach is then implemented to IT Service Management processes.

Keywords: risk assessment subjectivity decision making AHP ITSM

1 Introduction

Effective IT Services management (ITSM) proves to be impossible without managing inherent risks of ITSM processes.

Each company despite of its size and specifics encounters the need to manage various types of risk. Experience of largest international enterprises demonstrates that the company cannot reach stability and increase its efficiency when risk management process is not embedded into the management system of the company [1].

The key part of risk management is a decision making – efficiency of risk management process is directly dependent on ability of decision makers to make informed decisions [2]. But people tend to make wrong decisions. According to D.Hubbard [3], human errors related to subjectivity in decision making are one of ten main causes of ineffective risk management [3].

Thus finding risk management tools that would eliminate possible subjectivity of decisions to be made becomes an important issue. It seems appropriate to focus on risk assessment. During risk assessment, current threats and their impacts are identified, then identified risks are prioritized. Company management decides on risk response strategies based on risk assessment results, that is why well-informed decisions made during risk assessment are vital for efficiency of risk management process as a whole.

2 Approaches to risk assessment

There are a number of standards and methodologies designed to assist company management in developing risk management systems. The most widespread and universal standards are FERMA, ISO 31000:2009 and COSO II.

Despite of versatility, each of the documents is aimed at a specific goal, which causes the difference in types of risks and risk management tools described by them. However, one can identify similarities in risk assessment processes described by standards. Analysis of risk assessment approaches defined by COSO II, FERMA, ISO 31000 (Figure1) revealed that there are three basic tasks to be completed during risk assessment; those are risk identification, measurement and prioritization. Each task requires decision making – whether it is choosing a method for risk identification and measurement or ranging the identified risks. Choosing risk identification and measurement methods is a very particular problem as selection criteria strongly depend on company profile. As a result, methodologies and standards do not describe definite tools for choosing a method but provide general recommendations. On the contrary, there is a widespread tool used for risk prioritization offered by each of the documents listed above – that is a risk matrix. Columns of risk matrix describe the likelihood of risk occurrence and rows present the consequences - possible impact of risk occurrence. Impact assessment criteria can include financial, reputational, operational, compliance and other consequences. Companies typically define impact using a combination of these consequences given that different risks may have different impacts on the company (see an example of impact assessment scale in Table 1). However, usage of risk matrix has its disadvantages. L.A.Cox states that usage of risk matrix for risk evaluation has several limitations [4]:

- Typical risk matrices can correctly compare a small fraction (less than 10%) of randomly selected pairs of hazards;
- Effective resource allocation for risk countermeasures cannot be based on categories provided by risk;
- Risk matrices can mistakenly assign higher (or lower) qualitative ratings to quantitatively lower (or higher);
- Ratings derived from risk matrices may be subjective and dependent on judgements of a decision-maker.

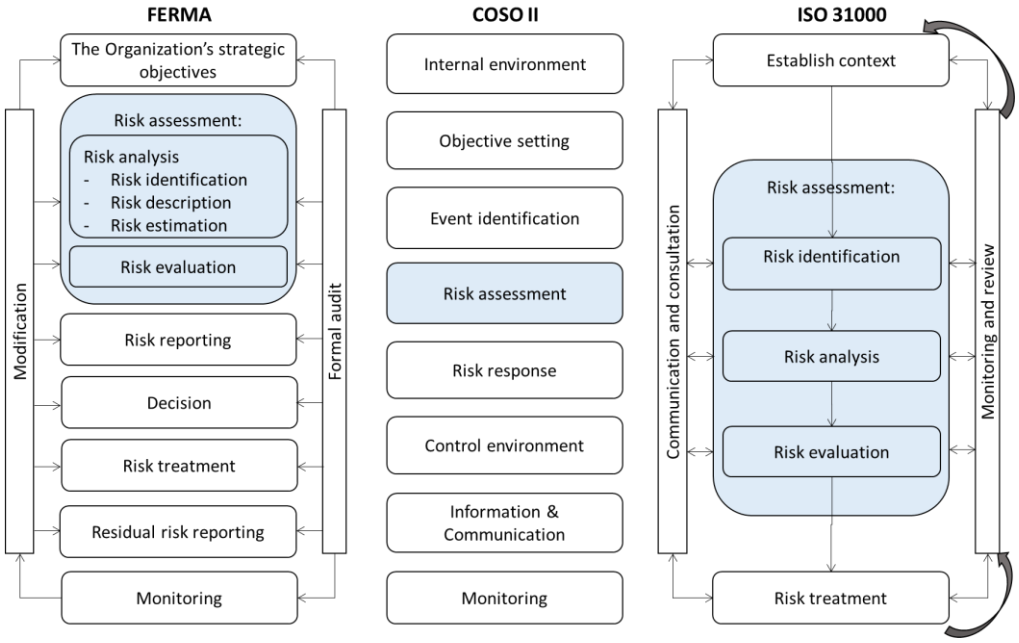

Figure 1 Risk management process in COSO II, FERMA, ISO 31000

The last two limitations listed above strongly affect the quality of decisions made by company management. They can be surpassed by developing a highly detailed risk assessment scale and by using risk measurement methods effectively. However, companies tend to develop risk matrices based on subjective judgements due to limited time and human resources (which is a quite common situation).

Obviously, standards and best practices in risk management do not suggest tools and methods to decrease subjectivity of decisions made during risk assessment. Nevertheless, such tools are well known in decision theory that offers a reasonable approach to decision-making under uncertainty, when the result depends solely on the preferences of the responsible person.

3 Decision making techniques for risk assessment

As consequences of risk occurrence affect various aspects of the company (and IT Service Management in particular), it is reasonable to use multicriteria decision-making methods for risk ranging. These methods would allow us to avoid usage of risk matrices and enable to range risks based on decision maker judgments.

Researches dedicated to decision making methods indicate that such methods (ELECTRE, TOPSIS, PROMETHEE, AHP, etc.) provide similar evaluation of alternatives being considered [5, 6]. So choosing a decision-making method entirely depends on the type of the problem faced by decision maker.

TABLE 1 Illustrative impact scale for risk assessment

Rating	Descriptor	Definition
5	Extreme	• Financial loss of $X million or more • International long-term negative media coverage; game-changing loss of market share • Significant prosecution and fines, litigation including class actions • Significant injuries or fatalities to employees or third parties, such as customers or vendors • Multiple seniors leaders leave
4	Major	• Financial loss of $X million up to $X million • National long-term negative media coverage; significant loss of market share • Report to regulator requiring major project for corrective action • Limited in-patient care required for employees or third parties, such as customers or vendors • Some senior managers leave, high turnover of experienced staff, not perceived as employer of choice
3	Moderate	• Financial loss of $X million up to $X million • National short-term negative media coverage • Report of breach to regulator with immediate correction to be implemented • Out-patient medical treatment required for employees or third parties, such as customers or vendors • Widespread staff morale problems and high turnover
2	Minor	• Financial loss of $X million up to $X million • Local reputational damage • Reportable incident to regulator, no follow up • No or minor injuries to employees or third parties, such as customers or vendors • General staff morale problems and increase in turnover
1	Incidental	• Financial loss up to $X million • Local media attention quickly remedied • Not reportable to regulator • No injuries to employees or third parties, such as customers or vendors • Isolated staff dissatisfaction

In order to select a decision-making method to support a risk prioritization process, we used quite general criteria for comparative evaluation of methods [7]:

- Possibility to use both qualitative and quantitative information about preferences of decision maker;
- Ability to quantitatively rank the alternatives to ensure clarity of the results and ease of interpretation;
- Ability to check the consistency of received decisions;
- Availability of mechanism to define a scale of evaluation criteria;
- Relative ease of use – there should be no need to involve experts or have a specific knowledge to apply the method.

We performed a comparative evaluation of methods for compliance with the selected criteria based on the analysis of studies on practical applications of multicriteria decision-making methods [5][6][8][9][10]. As a result we decided to apply AHP for risk assessment as it fully complies with evaluation criteria (see the results of evaluation in Table 2).

In this research we used AHP to assess the influence of risks on different aspects of IT Service Management.

TABLE 2 Decision making techniques for risk assessment

Criteria	AHP	ELECTRE	PROMETHEE	TOPSIS	MAUT
Quantitative and qualitative information					
Quantitative ranking of alternatives		×	(not all methods of the family)		
Consistency check				×	
Mechanism to define a scale of evaluation criteria		×	×	×	×
Ease of use		×			×

4 Applying AHP to ITSM processes risk assessment

Risk assessment model using AHP is applied to the results of IT control environment assessment project performed for a large company engaged in development and support of customized software, IT outsource and IT consulting. During the project compliance of internal control system to requirements of Sarbanes-Oxley Act was assessed. General methodology of control environment assessment was based on COSO II requirements to internal control system. As risk is an event preventing the process from achieving its goal, IT goals in accordance with Cobit 5 documents were used for risk identification.

As an interim result of control environment assessment project a register of risks inherent to the company was developed. For current research we chose to analyze risks in ITSM processes; in Cobit 5 documents these processes are described in "Deliver, Service and Suport" (DSS) domain. Risk assessment is performed only for those risks in DSS domain that were not mitigated by relevant control procedures at the time of the project and for which a risk response strategy is to be developed (see a list of risks in Table 3).

TABLE 3 Unmitigated risks in ITSM processes mapped to Cobit 5

Cobit 5 process	Risk #	Risk description
DSS01 Manage operations	IT.R2	Inability or delay in recovery of information systems due to inability to maintain recovery procedures or improper recovery.
DSS02 Manage service requests and incidents	IT.R3	Incomplete or untimely resolution of incidents and service requests due to incomplete registration of incidents and\or untimely processing of requests (including violation of SLA).
DSS03 Manage problems	IT.R3	Incomplete or untimely resolution of incidents and service requests due to incomplete registration of incidents and\or untimely processing of requests (including violation of SLA).
DSS05 Manage continuity	IT.R5	Unauthorized usage of information resources of the Company including introduction of changes to financial data due to granting unauthorized access or extended privileges.
DSS06 Manage business process controls	IT.R7	Incorrect operation of information systems due to (1) implementation of unauthorized or not fully tested changes to information systems; or (2) incorrect implementation of the change management cycle to newly developed systems.

Risks in ITSM processes are the alternatives to be ranked based on developed evaluation criteria. We used financial, reputational, operational and compliance consequences of risks as such criteria. Those are often used when developing a risk matrix and happen to be the most widespread. However, AHP does not limit a number of criteria to be used for assessment – one can evaluate a risk impact on a greater number of consequences if needed.

Problem of risk ranking in ITSM processes is shown as a hierarchical structure of objectives, criteria and alternatives in Figure 2.

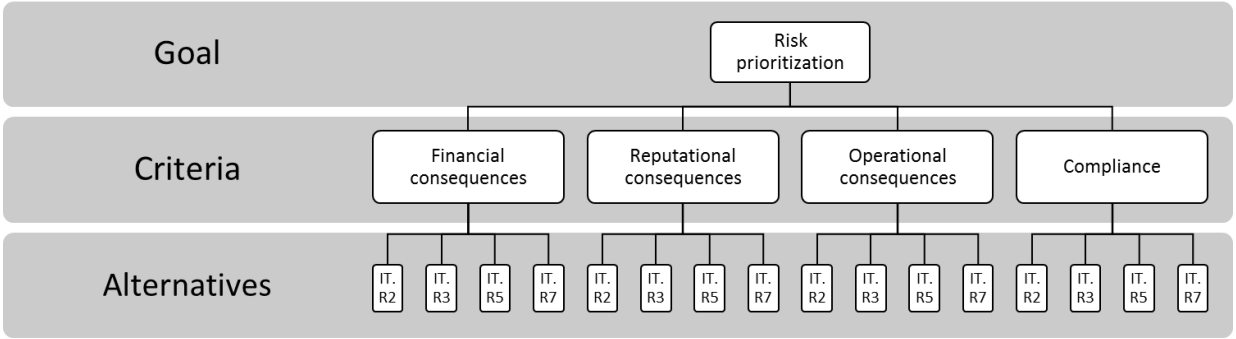

Figure 2 AHP risk assessment hierarchy

In our research the decision maker is a Head of IT Department in a company where control environment was assessed and unmitigated risks in ITSM processes were identified. Pairwise comparison matrix for defined criteria is developed based on judgements of the decision maker; it is worth to mention that priority of criteria is defined according to the impact on IT Department performance and not the performance of the whole company. Determining of global priorities of criteria through calculation of normalized principal eigenvector is performed using MATLAB R2014a (Version 8.3). Results of calculation are shown in Table 4.

TABLE 4 Pairwise comparison of risk assessment criteria

Criteria	Financial consequences	Reputational consequences	Operational consequences	Compliance	Weight of criteria
Financial consequences	1	4	2	1/3	24%
Reputational consequences	1/4	1	1/3	1/4	7.58%
Operational consequences	1/2	3	1	1/5	14.24%
Compliance	3	4	5	1	54.18%

Usage of pairwise comparison matrix provided us with a quantitative representation of decision maker's subjective judgements regarding importance of given criteria when assessing consequences of risk realization. Consistency index of the matrix is 7% which is an acceptable level (less than 10%) meaning that judgements of the decision maker are consistent and can be used in assessment.

Next step is making a pairwise comparison of alternatives (risks in ITSM processes) in context of developed criteria; this comparison is also based on decision maker's opinion and provides us with risk weights regarding specific criterion. Example of pairwise risk comparison in context of financial consequences is shown in Table 5; same comparisons were made regarding other criteria as well.

TABLE 5 Pairwise comparison of risks in context of financial consequences

	IT.R2	IT.R3	IT.R5	IT.R7	Risk weight
IT.R2	13%	26%	34%	7%	**13%**
IT.R3	5%	19%	13%	6%	**8%**
IT.R5	56%	6%	5%	59%	**46%**
IT.R7	26%	50%	48%	29%	**32%**

After determining risk weights with respect to each criterion we performed a comparison of risks based on global priorities of criteria shown in Table 4 and calculated composite risk weights (see Table 6 for results). As seen from Table 6, ranking of risks in ITSM processes after applying AHP to risk assessment is the following: firstly, risk response strategy has to be developed for risk IT.R5 as it has the biggest weight and thus the biggest influence on business activity of the company. Then risk response has to be developed for risk IT.R7; after that risks IT.R2 and IT.R3 need to be considered.

TABLE 6 Pairwise comparison of risk impacts on evaluation criteria

	Financial consequences	Reputational consequences	Operational consequences	Compliance	Composite risk weight
Weight of criteria	*24%*	*8%*	*14%*	*54%*	
IT.R2	13%	26%	34%	7%	**13%**
IT.R3	5%	19%	13%	6%	**8%**
IT.R5	56%	6%	5%	59%	**46%**
IT.R7	26%	50%	48%	29%	**32%**

5 Conclusion

Evaluating the results of applying a decision-making method is a nontrivial and hardly feasible task. Decision-making methods are applied in cases when there obviously cannot be a clear answer; these methods are designed to help a decision maker systematize his judgements and formalize the decision-making process. Thus, applicability of the concrete method is also decided by a decision maker based on ease of use, transparency and consistency of the method with natural course of thinking. AHP has several advantages – first of all, AHP enables a decision maker to take into account the human factor in a decision making process, including those cases when decision is made not by one person but a group of people. Secondly, AHP allows to quantitatively express the preference of one option over another. This, in turn, allows to fully identify preferences of the decision maker, and consistency check shows whether we can trust the results. The method is general-purpose as it can be applied to the task from any field. Thanks to hierarchical representation of the problem suggested by AHP, the decision maker can divide the problem into separate tasks and delegate them to several experts. Therefore, it can reduce the complexity of data preparation and the difficulty of application of the method which occurs when a large number of criteria and alternatives is assessed (in this case, the number of pairwise comparisons to be carried out increases drastically).

One way to develop our research is to revise evaluation criteria. As we stated earlier, risk is an event preventing the process from achieving its goal. Obviously, achievement of different goals brings different value to the company. AHP allows using multiple levels of criteria, so it seems useful to

define the relative importance of each goal and consequences influencing achievement of this goal, and the assess the risks. Moreover, it seems appropriate to automate the method and create a system that would interpret the results of the method in understandable terms. Currently, results obtained after applying AHP can be easily interpreted if we assess a relatively small number of criteria and alternatives; when assessing a bigger number of factors interpretation of the results with respect to each criterion becomes more complex.

Developed approach to risk assessment was reviewed at Enterprise Risk Services department of international company providing audit and consulting services. Peer review confirmed that currently experts use risk matrices for risk prioritization when developing risk management systems in the companies of different profiles. Risk evaluation is often carried out by voting of client's senior management regarding importance of different risks based on the prescribed scale. It was noted that using AHP for risk assessment would help to decrease the subjectivity of estimates and check the consistency of judgements of senior management. The approach was applied to results of finished projects; the approach was said to be adequate and recommended for usage in future projects on developing risk management system and assessing company risks.

References

[1] Martsinovskij D A 2009 Review of basic aspects of risk management *Das Management* **1**(11) 54-60

[2] Rabihah Md.Sum. 2013 *Risk Management Decision Making: Proc. ISAHP Kuala Lumpur, Malaysia* http://www.isahp.org/uploads/47.pdf */29 May 2015*

[3] Hubbard D W 2009 *The failure of management: Why it's broken and how to fix it* Hoboken New Jersey: John Wiley.

[4] Cox L A 2008 What's Wrong with Risk Matrices? *Risk Analysis* **28** (2)

[5] Salomon V A P 2001 *A compilation of comparisons on the Analytic Hierarchy Process and others Multiple Criteria Decision Making methods: some cases developed in Brazil Proc. 6th ISAHP Berne, Switzerland* http://www.isahp.org/2001Proceedings/Papers/033-P.pdf /4 Jun 2015

[6] Martowibowo S Y, Riyanto H 2011 Suitable Multi Criteria Decision Analysis Tool *Journal of KONES Powertrain and Transport* **18**(4) 273-81

[7] 2004 *Decision making technologies: analytical hierarchy process* http://citforum.ru/consulting/BI/resolution/ */30 Apr 2014 (in Russian)*

[8] Gerdes J W, Spero E 2013 *A Compact Review of Multi-criteria Decision Analysis Uncertainty Techniques* http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA582195 /16 May 2015

[9] Aruldoss M, Lakshmi T M, Venkatesan V P 2013 A Survey on Multi Criteria Decision Making Methods and Its Applications *American Journal of Information Systems* **1**(1) 31-43

[10] Velasquez1 M, Hester P T 2013 An Analysis of Multi-Criteria Decision Making Methods *Int. Journal of Operations Research* **10**(2) 56-66

[11] Perminov A A 2011 Qualitative risk assessment using analytical hierarchy process *Upravl uchet i finansi* **03**(27)

Authors

Vladimir Grekul, 1949, Sakhalin, Russia

Current position, grades: professor, National Research University Higher School of Economics, Moscow, PhD
University studies: Kiev Higher Engineer Aviation Training School of the Air Force
Scientific interest: IT management
Publications:90
Experience: has 40 years experience in design and implementation of information systems, has been working at NRU HSE since 2001 as Professor.

Nina Korovkina, 1947, Moscow, Russia

Current position, grades: Associate professor for the Information Systems and Digital Infrastructure Management department, National research university – Higher school of economics (Moscow, Russia)
University studies: Moscow institute of railway transport, engineer-mathematician specialization majoring in "Mathematical and computing devices"
Scientific interest: Design and implementation of information systems, IT project management
Publications: 39
Experience: worked in the Central economics institute for economics and mathematics (division of the Academy of sciences, Moscow, USSR) as well as in the Main computer centre of State planning committee. Since 1994 has been working in the National research university - Higher school of economics, took part in the projects carried out for the Ministry of Education, Ministry of Economic Development and Trade, Ministry of Information Technologies and Communications

Ksenia Korneva, 1993, Moscow, Russia

Current position, grades: Consultant, Deloitte & Touche CIS, ERS
University studies: Master of Business Informatics, National Research University – Higher School of Economics (Moscow, Russia)
Scientific interest: Risk management, internal control system review
Publications: 1
Experience: in 2012 Intern at Enterprise Risk Services, Deloitte & Touche CIS. Currently is a Consultant with three years of experience in projects related to Audit Support (IT audit), SOX-compliance and development of internal control system.