Choosing a Prioritization Method – Case of IS Security Improvement

Camille Salinesi, Elena Kornyshova

camille.salinesi@univ-paris1.fr, elena.kornyshova@malix.univ-paris1.fr
CRI, University Paris 1 - Panthéon Sorbonne
90, rue de Tolbiac, 75013 Paris, France
Economic Cybernetics Department, Saint-Petersburg Business and Finance State University
21, Sadovaia Str, 191023 Saint-Petersburg, Russia

Abstract. A number of multi-criteria decision-making methods can be used for prioritizing in different contexts. Our industry experience showed us that -at least in France and Russia- people are not aware of the existing prioritization methods and not able to select one when they are provided with a simple state of the art reference list. We therefore believe that a structured approach is necessary for guiding the systematic selection of a prioritization method. Our proposal consists in a process that helps the decision makers considering the different aspects of the problem at hand, and of the expected characteristics of the required method. The approach is illustrated with the example of a prioritization to be made for improving business and IS security in the banking sector. The selected method is chosen among: MAUT, AHP, Outranking, weighting methods, expert classification and fuzzy methods.

1. Introduction

Although multi-criteria decision-making methods have shown their qualities since over 30 years [1], our experience with the industry is that they are still not well known in the industry. Each prioritization method is able to deal with problems with specific characteristics. For instance the number and nature of the alternatives, of the decision criteria, the presence of multiple stakeholders with different viewpoints. Besides, the existing methods have different characteristics such as complexity or ability to deal with quantitative or qualitative criteria.

Our assumption is that a process guiding the selection of a decision-making method should take into account several aspects of the situation at hand. The proposed approach copes with these different aspects using a structured benchmarking grid.

The rest of the paper is presented as follows: section 2 gives an overview of the approach, which is detailed illustrated in section 3 with an example of IS Security Improvement. The concluding section discusses related works and research perspectives.

2. Overview of the proposed approach

As Fig. 1 shows it, our guidance is based on a process organized into 4 phases and resulting in the application of a prioritization method for the problem at hand. The goal of the *initiation* phase is to define the nature of the multi-criteria problem. Once the problem defined, the method proposes to *identify candidate methods* (phase 2), *evaluate* their ability to cope with the multi-criteria problem (phase 3), then *select* the most adequate method(s) (phase 4). Phases 2, 3 and 4 are iterative as several phases can match the problem at hand (in which case a more detailed analysis is required) or on the contrary none of the candidate methods matches the problem perfectly (another choice must then be made, either in a least worst strategy, or based on a different choice of candidate methods).

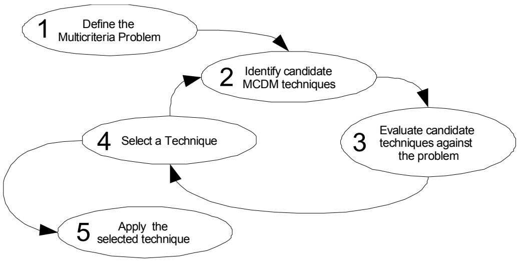
1 Define the Multicriteria Problem
2 Identify candidate MCDM techniques
3 Evaluate candidate techniques against the problem
4 Select a Technique
5 Apply the selected technique

Figure 1: Overview of the proposed approach

3. Example of application: business security planning

Our example is situated in the context of the Bâle II law which obliges financial organizations to invest in risk reduction (from power supply shutdown in a building to natural catastrophe or terrorist attack) by applying Business Continuity Plan (BCP) elaboration methods such as [2,3]. We observed that the first questions raised when applying such a method in practice is "what should be protected first?", "what should be restored first?", "which asset, operation or application represent important essential risk factors?", "which are the vital business processes for the security of the enterprise and of its IS?" and thereafter more fundamentally "how should these choices be made?". The following sub-sections illustrate the choice of a prioritization method in this context.

3.1 Defining the Multi-criteria Problem

Our experience showed us that the traditional multi-criteria formulation of a prioritization problem [4] is useful to understand a method, but not enough precise to select a method among others. Based on a state of the art research [5], we developed a benchmarking grid that helps defining the multi-criteria problem in more details. The grid is made of 15 different facets organized into four orthogonal dimensions, namely context, process, form, and object.

- The *context* dimension gathers 5 characteristics of the situation of use of the method: (i) the problem calls for a choice (ii) a ranking, (iii) or a sorting, (iv) new alternatives can emerge, and (v) there are multiple viewpoints.
- The *process* dimension gathers 4 characteristics of the methods' expected way of working: (i) the approach for defining evaluations (either unique criterion of synthesis, outranking or iterative), (ii) for defining the decision criteria (either without weighting, with weighting and interdependencies, or simple weighting), (iii) the ability to have deal with different scales for the evaluations, and (iv) easiness of use (easy, medium or difficult).

- The *form* dimension characterizes how the method is described. This dimension gathers two characteristics: (i) notation (textual explanation, mathematical formula, function), and (ii) tool to indicate if a COTS is available to support the method.
- The *object* dimension gathers 4 characteristics of the alternatives that can be prioritized: (i) type of the data that can be considered (either quantitative or qualitative), (ii) number of alternatives that can be considered using the method (either large or small), (iii) ability to take into account incompatibilities and conflicts between alternatives, and (iv) hierarchicality (ability to deal with alternatives organized hierarchically).

In the context of our example, it was chosen to focus on the decision of what should be secured first. This ranking question is fundamental as its answer will result in the selection of the key processes that will be crucial for the functioning of the enterprise when a crisis situation arises. The criteria put forward by our chief executive are: costs, customer value, contribution to strategic objectives, and risk of the threat (a more complete list would be elaborated in reality, we limit our example to these criteria for the sake of space). These criteria have different scales: cost and value are absolute numerical data, whereas risk is a ratio, and contribution to strategic objectives a nominal scale. Besides, the analysis involves multiple stakeholders with different -and sometimes contradictory- viewpoints (for instance the financial director wants to reduce costs is opposed to the CIO who tries to increase IS security).

3.2 Identifying Candidate MCDM methods

Six families of MDCM methods can be considered: MAUT [6], AHP [7], outranking methods [8], weighting methods [9], expert classification [10], and fuzzy methods [11]. These are not detailed here into for the sake of space. However, an overview is given by the table below. All the methods were considered in the rest of the example.

Dimension	Facets	MAUT	AHP	Outranking	Weighting	Fuzzy methods	Expert Classification
Context	Problematic, choice	Yes	Yes	Yes	Yes	Yes	No
	Problematic, ranking	Yes	Yes	Yes	Yes	Yes	No
	Problematic, sorting	No	No	Yes	No	Yes	Yes
	Treatment of a new alternative	Yes	No	Yes	Yes	Different	Yes
	Taking into account of the multi-views	No	No	Yes	No	Different	Yes
Process	Approaches for defining evaluations	UCS	UCS	Outranking	UCS	Different	Iterative
	Approaches for decision criteria weighting	Yes, no interdep	Yes, interdep	Yes, interdep	Yes, no interdep	Yes, interdep	No
	Taking into account of various scales of criteria	Yes	No	Yes	No	Different	Yes
	Easiness of use	Difficult	Easy	Medium	Easy	Difficult	Difficult
Form	Notation	Utility function	Balanced sum	Textual	Weighted sum	Different	Textual
	Tools	No	Yes	Yes	Yes	Different	Yes, medical domain

Dimension	Facets	MAUT	AHP	Outranking	Weighting	Fuzzy methods	Expert Classification
Object	Data type	quan, qual	quan, qual	quan, qual	quan	quan, qual	quan, qual
	Number of alternatives to be treated	Great	Small	Great	Great	Different	Great
	Treatment of incompatibility, alternatives conflicts	Yes	No	Yes	No	Yes	No
	Hierarchicality	No	Yes	No	No	Different	Yes

Table 1: Overview of the panel of methods considered in the example

3.3 Evaluating Candidate methods

The goal here is to identify which candidate method satisfies all the characteristics that have been defined at phase 1. The principle is to identify for each characteristic the method that are satisfactory.

For instance, in our example: (i) all the considered methods deal with the problem at hand (ranking), (ii) AHP is not able to treat the apparition of new alternatives, (iii) only Outranking Fuzzy MCDM and expert classification are able to deal with multiple viewpoints, and (iv) only Outranking and Fuzzy MCDM are able to deal with conflicting alternatives.

3.4 Selecting and applying a method

Of course, it can happen that there are several or no method that satisfies all characteristics. In this case, another cycle of evaluation must be achieved. Several strategies are available: either other methods are considered, or some of the required characteristics are added or removed, or the characteristics are ranked by order of importance.

Both Outranking and Fuzzy MCDM satisfy all the example's characteristics. The chief executive decides to choose Outranking because it is less complicated. Although this criterion was not defined in the initial phase of the process, it is useful to rapidly make the final decision. Five recommendations result from this choice: (i) introduce ELECTRE II in the definition of the BCP to target clearly defined ROIs, (ii) use multiple criteria so as to optimize decisions, (iii) adapt results when there are changes (iv) take into account criteria interdependencies and alternatives conflicts, and (v) take multiple viewpoints into account.

4. Conclusion: related works and perspectives

As defined by [12] in the context of method engineering, or [13] in the context of COTS selection, choosing among a panel of methods and tools available on the market is not an easy task. Our observation of the industrial usage of MCDM methods in French and Russian industry showed us that there is a lack of guidance for choosing the method that best responds to the problem at hand. We propose a structured approach that guides the selection of a prioritization method. The approach is based on a benchmarking grid to structure problem definition and guide the analysis of ability of selected methods to comply with expected characteristics. New dimensions, facets and sub-facets could be added to the grid to provide support for finer-grain analysis. We also admit that the quality of the result depends on the quality of the state of art and positioning of each method on each facet.

The approach was developed based on practical experience in the industry[1]. We believe it could be generalized to guide method chunk selection (e.g. as an alternative to J. Ralyté's similarity based approach). More guidance is however needed: to adapt the approach to different contexts of use as well as to improve its efficacy. We intend to evaluate its efficiency and genericity by applying it to different prioritization problems: portfolio management, prioritization of evolution requirements, and tendering processes.

5. References

[1] P. Berander. Requirements Prioritization. In Engineer'ing and Managing Software Requirements. (Eds A. Aurum, C. Wohlin). Springer. 2005.

[2] Moulton B. *Bâle II : Risques opérationnels et sécurité des informations*, http://information-integrity.symantec.fr/article.cfm?articleid=270, 2005.

[3] S. Petrenko, O. Remizova. *Avez-vous un plan?* Directeur IT, 76-81, 2005.

[4] C. Zopounidis. *Décisions financières et analyse multicritère*, Encyclopédie de Gestion, (Simon, Y. and P. Joffre, Eds), Economica, 2e Edition, Paris, 915-925., 1997.

[5] E. Papadacci, C. Salinesi, L. Sidler. *Panorama des approches d'arbitrage dans le contexte de l'urbanisation du SI, Etat de l'art et mise en perspective des approches issues du monde de l'ingénierie des exigences.* special issue ISI Journal, 2005.

[6] R.L. Keeney,H. Raiffa. *Decisions with Multiple Objectives: Preferences and Value Trade-Offs.* Cambridge University Press, 1993.

[7] T.L. Saaty. *The Analytic Hierarchy Process.* NY, McGraw Hill, 1980.

[8] B. Roy. *Multicriteria Methodology for Decision Aiding*. Dordrecht: Kluwer Academic Publishers, 1996.

[9] R.L. Keeney. *Foundations for Making Smart Decisions*, *IIE Solutions*, 31, No. 5, 1999.

[10] F. Moisiadis. *A Framework for Prioritizing Use Cases.* Joint Research Centre for Advanced Systems Engineering, Australia, 2005

[11] S. Zhang. X. Liu. *Realization of Data Mining Model for Expert Classification Using Multi-Scale Spatial Data.* ISPRS Workshop on Service and Application of Spatial Data Infrastructure, Hangzhou, China, 2004.

[12] J. Ralyte, and C. Rolland. *An assembly process model for method engineering*. Proceedings of CAISE'01, Interlaken, Switzerland, June 2001.

[13] C. Ncube, N. Maiden. *Guiding Parallel Requirements Acquisition and COTS Software Selection.* Proceedings of RE'99, Limerick, Ireland, June 1999

[1] Elena Kornyshova was control manager for several years in different companies before starting research