The Applicability of Multi-Criteria Decision Aiding Methods to Risk Management

Ana Sara Costa¹, Ricardo Vieira², Cristina Verdasca², and José Rui Figueira¹

¹ CEG-IST, Instituto Superior Técnico, Universidade de Lisboa, Lisbon, Portugal
² INESC-ID, Instituto Superior Técnico, Universidade de Lisboa, Lisbon, Portugal
{anasaracosta, rjcv, cristina.verdasca, figueira}@tecnico.ulisboa.pt

Abstract. This paper addresses the problem of the design and development of a framework for the exploitation of Multi-Criteria Decision Aiding (MCDA) methods in risk management scenarios. MCDA is a branch of Operational Research, which deals with decision aiding for decision-makers in situations involving multiple criteria. MCDA offers a large range of methods to deal with the situations at hand in decision processes. Due to the considerable complexity of the interactions or amount of computation required by some MCDA methods, applying them without software support is hardly imaginable. Implementing an easy-to-use software solution that simultaneously provides advanced support for using the MCDA method, without requiring unnecessary expertise from the user, presents a new practical challenge from the viewpoint of information technology. This paper addresses that problem, in the scope of a risk management process.

Keywords: Multi-Criteria Decision Aiding · Decision Support Systems · Risk Management

1 Introduction

This paper makes the case for a new web-based integrated framework to explore Multi-Criteria Decision Aiding (MCDA) methods in the domain of risk management.

MCDA is a branch of Operational Research that deals with various problematics (choice, ranking, sorting, or description) involving multiple criteria. It aims at helping decision-makers during the decision aiding process. In this field, over the last years, several MCDA methods have been developed. When applying some of those MCDA methods, we have to deal with a considerable complexity of the interactions and a great amount of computation. Most of the software that is available as open-source or for reuse has been developed by academic researchers, both general-purpose software and application-specific software. One requirement of the implementation of the software is to ensure that users having a little experience are also able to use it. Consequently, the challenge is implementing an easy-to-use software able to simultaneously provide advanced support for using the MCDA method, while a certain expertise from the user to use it is not necessarily required.
However, a critical issue in this kind of software solutions is the trade-off of their focus in either the method or the application. Software solutions focused mainly in the method tend to be very flexible for that purpose, but hard to use to those not skilled in the method (the mechanics of some methods can be really not obvious in a first glance). On the other side, a Decision Support System (DSS) focused exclusively on the specific requirements of a specific domain of application and hiding too much the details of the decision support method, is hardly reusable for other domains. The purpose of this work is to motivate for the potential of development of a generic MCDA framework as a reusable DSS component for the domain of risk management, by providing an early analysis of the problem.

In the following two sections, we describe the fundamental concepts of MCDA, and provide the main references to documented sources of MCDA tools. In the next section, we present the fundamental concepts of risk management. Next, we provide an analysis of the applicability of the MCDA to the risk management domain. In section 6, we refer the main MCDA methods already identified as relevant for that domain, and the principles for a software solution implementing MCDA methods for risk management that should be taken in consideration. Finally, in section 7, we provide some concluding remarks.

2 Fundamentals of MCDA

MCDA aims at helping a decision-maker or a group of decision-makers during the decision aiding process, which usually is assisted by one or more decision analysts [1]. In organizations, a plethora of different decision making situations can arise. Sometimes, those situations can be complex, especially when they cover information of conflicting nature reflecting different points of view and requiring multiple expertise, thus the involvement of several actors in the same process. In order to reach the best possible results, such multidimensional nature of the problems should be considered, when possible, during the decision making process.

According to a particular decision aiding context, having tools that allow to select, to rank or to assign to categories the objects of a decision (actions, options or alternatives), can be a valuable aid. In the context of MCDA, various methodologies, methods and techniques have been developed, which can integrate many different types of information, in order to lead to better informed decisions (see, for instance, [2]).

The basic idea of using an MCDA method is to assess the performance of actions according to multiple criteria, taking into account the preferences of the decision-maker(s) in the decision process. All actions are simultaneously evaluated under a set of relevant, and typically heterogeneous and conflicting criteria. Furthermore, the actions must be evaluated on a coherent family of criteria and consistent methods [3].

In an overview of the core concepts:

“Decision aiding is the activity of the person who, through the use of explicit but not necessarily completely formalized models, helps obtain elements of responses to the questions posed by a stakeholder of a decision process. These elements work towards
clarifying the decision and usually towards recommending, or simply favouring, a behaviour that will increase the consistency between the evolution of the process and this stakeholder’s objectives and value system.” [3].

In this sense, a generic decision aiding process consists of four basic steps:

- a representation of the problem situation;
- a problem formulation;
- an evaluation model;
- a final recommendation [4].

It should be noted that the MCDA model must be co-constructed through the interaction between all the actors of the process, namely the decision analyst(s) and the decision-maker(s). This interaction ensures that the preferences of the decision-maker(s) are properly represented in the model.

According to [1], there are four main types of problematic:

- Choice problematic: it aims to select a set of ‘good’ actions in such a way that it is possible to choose the single best action;
- Sorting problematic: it aims to assign each action to one or more predefined categories;
- Ranking problematic: it aims to rank the set of actions (the order can be complete or partial);
- Description problematic: it aims to describe actions and their consequences.

3 Overview of MCDA tools

The application of MCDA methods needs to be supported by appropriate software solutions. For example, some MCDA methods require a large amount of computation, while other methods may also require support for the different phases of the decision aiding process (e.g., structuring of the problem, building of the model, analysis of the results, etc.).

Several software solutions have been developed to support the application of MCDA methods in real-world decision situations. A directory of MCDA software is provided at the web page of EURO Working Group on Multiple Decision Aiding (EWG-MCDA).

In [5], we can find an overview of existing MCDA software. In [6] are present MCDA methods that have a supporting software available along with the corresponding software description and implementation. MCDA software can cover different phases of the decision aiding process. and, in general, the basic structure of the MCDA process can be found practically in all the software available [5].

Various multiple criteria decision support software have been developed according to the type of the decision situation or the area of application. It is possible to find

1 Available at http://www.cs.put.poznan.pl/ewgmcda/index.php/software
MCDA software solutions available on the Internet, which can be used online or can be downloaded. Besides single software, resource collections can also be found [6]. Indeed, a variety of software that implements MCDA methods is available, both general-purpose software and application-specific software, and also in reusable open-source solutions.

4 Fundamentals of Risk Management

Risk management (RM) is defined as the “coordinated activities to direct and control an organization with regard to risk” [7]. Risk is “the effect of uncertainty on objectives” [7]. Uncertainty refers to “possible deviations from the expected” [8]. Therefore, a RM process is a set of activities required to manage possible deviations that can affect the achievement of objectives. The deviation can have a positive or negative effect on the objectives, i.e., the risk can possess a threat to the achievement of an objective or an opportunity to be explored. For example, the use of an innovative method in any business practice can be associated with the negative risk of using a non-tested and non-proved method, but also with the positive risk of increasing competitiveness on the market.

RM is increasingly recognized as an essential activity in any business and field of activity. Because of the diversity of contexts where RM can be applied, several RM frameworks exist. Depending on the context of application, specialized frameworks can recommend different techniques and methods for the activities of the RM process. The main technical references recognized nowadays as relevant for the support of a RM process independently of its context, are the historic COSO Enterprise Risk Management (ERM) Framework [9] and the ISO31000 family of standards.

4.1 COSO Enterprise Risk Management

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) issued in 2004 the COSO ERM Framework [9], intended to manage the existent uncertainty on organizational entities.

COSO ERM recognizes that entities in an organization exist to provide value for its stakeholders and that their value is maximized when their return value is balanced with their related risks [9]. As shown in Fig. 1, the COSO ERM framework is visually represented as a cube with three dimensions: the top dimension depicts the four objectives of the framework, the eight rows on front represent the activities of the RM process and the third dimension symbolizes the entity and its units.

The objectives of the ERM are categorized into [9]:

- “strategic, i.e., the high-level goals of the organization”;
- “operations, i.e., the goals related to the “effective and efficient use of the entity’s resources”;
- “reporting, that refers to communication and consultation goals”;
• “compliance, goals related with compliance to the regulatory environment of the organization”.

Fig. 1. COSO Enterprise Risk Management Framework [9]

The COSO ERM process comprise the following main activities [9]:

• Internal Environment, responsible for setting the risk culture of the organization, i.e., defining the risk appetite (the amount of risk the organization is willing to undertake), the commitment of the organizations’ entities, the available resources, etc.;
• Objective Setting, which consists on identifying the organization objectives;
• Event Identification, that involves the identification of risks (and their sources) that may affect, positively or negatively, the objectives identified above;
• Risk Assessment, where the identified risks are analysed in terms of their likelihood and impact;
• Risk Response, that involves the identification of possible risk responses (controls) to modify the risk likelihood and impact;
• Control Activities, where the risks responses selected in the previous activity are implemented;
• Information and Communication, where all the risk information is captured, structured and communicated to all relevant stakeholders;
• Monitoring, that consists on the implementation of monitoring procedures and practices to assure that modifications are made as necessary.


ISO 31000:2009 [7] defines a RM vocabulary, the guidelines for a RM framework and a generic RM process. The RM vocabulary is taken from ISO/IEC Guide 73 [8] – a guide that aims to define basic RM concepts and terms that are used across several contexts and domains. According to it, risk is “often characterized by reference to potential events and consequences, or a combination of these”. An event is defined as the
“ocurrence or change of a particular set of circumstances”. Its outcome and the way it affects objectives is defined as the consequence of the event. One of the main contributions of ISO 31000:2009 is the definition of a generic RM process, as illustrated in the Fig. 2.

Even though it is previous to ISO31000:2009 [9], COSO ERM claims to be aligned with its principles.

The process defines that the organization should start by the activity of establishing its context, i.e., defining its objectives for the RM, and define the internal and external factors that can influence the process. The process can then follow with the activity of risk assessment, comprising three main sub-activities:

- Risk identification, that involves the identification of “sources of risk, areas of impacts, events and their causes and their potential consequences” [7];
- Risk analysis, where attributes are estimated by, for example, assessing the likelihood of the events or the impact of their consequences;
- Risk evaluation, where, based on the outcomes of risk analysis, the stakeholders make an informed decision regarding which risks need treatment.

The activity of risk treatment comprises the definition and implementation of the controls that will modify the risk.

Finally, the process defines that through the aforementioned activities, it is vital that all outputs are constantly monitored and reviewed to ensure the correctness of the data, and also that all relevant stakeholders are consulted during the several RM activities.
5 The relevance of the MCDA methods to risk management

COSO states that one of the main goals of ERM is to provide rigor to the identification and selection among several alternative risk responses. However, according to COSO, one limitation is that ERM is subject to human judgement that can be faulty. Therefore, COSO recommends that risk decisions should be based on strong and pre-defined criteria that would justify and reduce the complexity of the decision-making in ERM. Therefore, although COSO does not explicitly recommend MCDA methods, it reinforces the need of defining suitable criteria to support decision-making – a goal of MCDA methods.

ISO 31000:2009 states that to achieve the goals of risk assessment activities (see Fig. 2) a plenitude of techniques can be used. Those techniques can differ in terms of purpose and benefits and can require different resources and capabilities to implement. Therefore, the decision of which techniques to choose is highly dependently on the context of application. To assist the decision, the ISO/IEC 31010:2009 [10] – Risk Assessment Techniques complements the ISO 31000:2009 [7] by describing 31 techniques to perform risk assessment. Each of these techniques is described regarding its suitability (strongly applicable, applicable, and not applicable) for risk identification, risk analysis and risk evaluation. One of the recommended techniques is MCDA, which according to this source is a strongly applicable technique for risk analysis and applicable to risk identification and risk evaluation. ISO/IEC 31010:2009 also includes a generic description of MCDA, and refers those methods can be used for [10]:

• “Comparing multiple options to determine preferred and potential options and inappropriate options”;
• “Comparing options where there are multiple and sometimes conflicting criteria”;
• “Reaching a consensus on a decision where different stakeholders have conflicting objectives or values”.

In the literature, it is possible to find examples of MCDA methods supporting risk management decisions [11,12,13,14,15]. However, the suitability of the methods is explained with regards to a specific problem of the context of application hindering the extrapolation of the solution to similar problems in other contexts.

6 Principles for a MCDA framework for Risk Management

MCDA methods are considered a suitable option for all the activities of risk assessment, due to its ability to support for decision-making in a context of coexistence of multiple classes of stakeholder, and therefore of multiple criteria – a common scenario in RM. Risk managers use several types of information in order to make decisions [16], namely:

1. The definition of the context where the risk management process is implemented;
2. Risk factors in order to estimate risk metrics in risk analysis in that context;
3. Control aspects in order to decide within alternative treatments in risk evaluation.

Regarding limitations, MCDA is dependent on a strong selection and definition of decision criteria – a task that can be challenging. Additionally, the use of an MCDA method might not reach a conclusive or unique solution to a problem, and criteria weights when poorly established can hamper the trustworthiness on the decision. The relevance of this potential, along with these potential limitations, are the main motivations for a goal of a carefully designed software framework for this purpose. This statement can be pointed as the first conclusion of this analysis. Besides the technical aspects, the role of the decision-maker in the decision aiding process and the user-friendliness of the interface should be also considered in implementing MCDA software. An additional requirement of the framework is enabling people that are not very familiar with MCDA methods could also be able to use it.

6.1 MCDA for classification in Risk Management

Concerning the input for the main functional requirements, a relevant challenge in RM is classification. In the context of RM, classifying risk factors into different risk categories (i.e., risk classification problems) are required for a wide range of areas, such as finance, project management, information security management, etc. Classification problems refer to the assignment of some actions into predefined categories (classes or groups), which are defined according to the preferences of the decision-maker(s) [17]. In the context of MCDA, we deal with an ordinal (sorting) or a nominal classification problem, depending on whether the categories are ordered or not, respectively. In the case of categories are defined a posteriori, we deal with clustering problems, and the categories can be called clusters [18]. Accordingly, risk classification problems can be treated as an ordinal classification problem (sorting). In conclusion, risk managers have to deal with sorting problematic decisions.

The importance of classification problems in various areas has motivated the development of a plethora of MCDA methods for constructing classification models, especially to provide decision support for real-world sorting problems (see, for instance, the state of the art reported in [19]). Several methods have been developed for sorting problems, such as UTADIS [20], ELECTRE TRI [21,22], ELECTRE TRI-C [23], ELECTRE TRI-nC [24] and SMAA-TRI [25], among others.

6.2 MCDA for eliciting risk criteria and risk factors

A risk register (also commonly referred as “risk log”) is a fundamental risk management tool. Its purpose is to be the repository for all the risk information, comprising the registration of each risk and the additional information about its aspects, such as risk concepts, metrics, stakeholders, controls (mitigation measures), etc. In order to be efficient and affective, that generic concept must be tailored to each specific use. For this purpose, it is fundamental the first activity of the RM process, the “Establishing the context”.

The challenges, in the scope of the RM activity, of the definition of the context, and within that, of the definition of the risk criteria, are stressed in [7]:

“The organization should define criteria to be used to evaluate the significance of risk. The criteria should reflect the organization’s values, objectives and resources. Some criteria can be imposed by, or derived from, legal and regulatory requirements and other requirements to which the organization subscribes. Risk criteria should be consistent with the organization’s risk management policy (see 4.3.2), be defined at the beginning of any risk management process and be continually reviewed.

When defining risk criteria, factors to be considered should include the following:

- the nature and types of causes and consequences that can occur and how they will be measured;
- how likelihood will be defined;
- the timeframe(s) of the likelihood and/or consequence(s);
- how the level of risk is to be determined;
- the views of stakeholders;
- the level at which risk becomes acceptable or tolerable; and
- whether combinations of multiple risks should be taken into account and, if so, how and which combinations should be considered.” [7].

Fig. 3 shows an example of a very simple domain model for a generic risk register (in the form of a UML class diagram). In this example, we can already realize several risk factors that are not always possible to quantify objectively, thus potentially motivating the use of MCDA methods to capture the knowledge of specialists. For example:

- Likelihood of events: knowledge about hazards and sources of risk have been consolidated for several domains (e.g., natural disasters, social behaviours, etc.), making it possible to use in some way reliable predictive models. However, that is true for only a limited number of phenomena, leaving the estimations in many other domains to the implicit knowledge and perception of experts;
- Value of an objective: the real value of a business objective or asset is not always only its book value. Frequently, a first order impact on an intangible asset (as for example, reputation) triggers higher order effects in the business that can be perceived by the experts in the business, but hard to make explicit and quantify.

For scenarios comprising challenges as described ahead, the precise quantification of the risk factors is not always possible, thus it is common the use of qualitative (or semi-qualitative) scales, which can be provided directly by an available expert, or as results of, for example, the use of MCDA processes. In other words, MCDA can aid risk managers to make better informed decisions, by adopting one of the four problematics (see section 2). Besides the sorting problematic usually arises, risk managers typically face also decision situations regarding choice and ranking. Moreover, although the description problematic is included in each of the other three ones, it can be considered as a separate contribution to make the information concerning risk factors and their
consequences (or risk criteria) more explicit. For instance, risk managers may be interested in developing an ordering procedure that ranks the risk factors in order of decreasing priority.

Fig. 3. A generic domain model for a simple risk register

Note that real life scenarios in risk management can really be even more complex. Fig. 4 illustrates a more sophisticated domain model for a risk register, where we can identify a much larger number of risk factors (e.g. residual risk of a control, exposure of a vulnerability, likelihood reduction of a control, among others). The value of a risk register considering all these concepts would be very high, but is very unusual to find RM contexts using this level of complexity, as the necessary costs of information management might make it too expensive for the expected benefits. However, that can change dramatically if proper software tools can emerge to manage risk registers at this level, thus reinforcing our proposal for that purpose.

Fig. 4. A generic domain model for a sophisticated risk register
7 Conclusions

In this paper, we intend to address the problem of the development of a new web-based integrated framework for the exploitation of MCDA methods, in the context of RM. The main contribution of this paper is to provide an analysis of the principles that should be taken into account for a software solution implementing MCDA methods, in the risk management domain. Moreover, our purpose is also to motivate for the potential development of a generic MCDA integrated framework for RM. The analysis present herein illustrates the applicability of the MCDA methods to RM, and improves the scope of the development of a framework of MCDA methods as a component of a DSS to RM.

This paper shows that various MCDA methods may be useful in RM scenarios. An analysis of the existing MCDA methods suitable for RM requirements can be a future avenue research. Future research could take advantage of the opportunities offered by such methods to RM, by designing and developing a new web-based integrated framework to support RM processes.

Acknowledgments. This work was supported by national funds through Fundação para a Ciência e a Tecnologia (FCT) with reference UID/CEC/50021/2013. The first author acknowledges the financial support from Universidade de Lisboa, Instituto Superior Técnico and CEG-IST (Bolsa de Doutoramento).

References


