

Supporting Decision-Making with the Tools of Risk Management

István Fekete

Corvinus University of Budapest

istvan.fekete@uni-corvinus.hu

SUMMARY

This year the Directives (hereinafter referred to as: Directives) to implement Act CXXII of 2009 and Government Decree 339/2019 on the internal control system of companies in public ownership were issued. One focal element of the internal control system is illuminated in the first part of the study in detail, based on the theoretical background of establishing the risk management system and the relevant standards and academic literature. It turns out from the first part that the key added value of risk management is the support given to decisions made at different levels. The study therefore presents a potential approach to demonstrate how risk management may be used efficiently to support strategic and project level decision-making, if there are no past data available, or not in sufficient quantity. In the second part of the study the author shows the experiences of the implementation of the risk management system - pursuant to the Directives - via the example of a large company. Relying partly on this and using his own experiences of many years the author specifies the factors supporting and hindering the implementation of the risk management system. According to his intention, the author specifies messages that may be helpful to practising experts to avoid the detection, evaluation and management of risks becoming administrative tasks. They must instead contribute to the long-term successful operation of the using organisation.

KEYWORDS: internal control system, integrated risk management, compliance, practical experiences

JEL CODES: A10, C13, C15, C41, M10, M21

DOI: https://doi.org/10.35551/PFQ_2022_s_1_2

Naturally, it is very important that every company operates in compliance with the relevant legal regulations pursuant to the contents of the Directives. It is, however, equally important to make decisions at strategic, operative and project levels, which guarantee the success of the given organisation in the long run. One aspect of this is the implementation of risk-based decision processes, which will be the focal point of the present study pursuant to MSZ ISO 31000:2018 standard in effect in Hungary since 1 January 2019.

RISK MANAGEMENT PURSUANT TO MSZ ISO 31000:2018 STANDARD

The standard states that risk management is an organic part of responsible corporate governance, thus it affects the management activity at the different levels of the organisations.

Principles related to the establishment of the risk management system

The study details the principles facilitating the implementation of targets based on the standard. Using his over 20 years of practical experience, the author makes explanatory comments to every single principle, which may guide the readers in selecting what to pay attention to when they wish to implement the risk management system at a given organisation.

The already referenced standard states that the purpose of risk management is value creation and value preservation. This purpose may be implemented with the fulfilment of the following principles:

▶ *‘Risk management must cover every activity of the given organisation.’* Translating this to

the language of practice, it means that from strategy creation, through the preparation and implementation of projects facilitating the implementation of the strategy, to the processes describing the daily operation, exploring and evaluating the risks is a must everywhere, with special attention given to the potential interactions between the risks arising at different levels.

▶ *‘The structured and comprehensive approach of risk management contributes to reaching consistent and comparable results.’* Translating this yet again to the language of practice it means that the assessment and the management of risks are not one-time activities, they must be repeated from time to time in order to backtest the efficiency of risk management. This may only be ensured if the structure of the assessments performed at different times does not change.

▶ *‘The involvement of the concerned parties in appropriate manner and time facilitates the sharing of their knowledge, opinion and intuition. This will result in higher level of awareness and better prepared risk management.’* This principle thus prescribes, on the one hand, the involvement of experts with appropriate knowledge and experience in the subject of the given assessment from as wide range as possible in the assessment and management of the risks. On the other hand, it is necessary to establish forums ensuring the more efficient way of letting experiences and knowledge surface.

▶ *‘Risks may change, new risks may arise or cease to exist as a result of the changes of the environment. The task of risk management is to forecast, show, accept and react to the changes and the related events in appropriate time and manner.’* This principle also suggests that the assessment of risks is not a one-time activity. This principle, however, also has another key message, namely that it is worth recognising the potential risks as early as possible, because

it is the only opportunity to manage them efficiently. Even if we do not recognise them, they may still arise. If a risk takes us by surprise, we may not be able to select the most efficient way of managing it.

▶ *Inputs used during the management of risks are based on past information and information available at the time of the assessment or on future expectations. This is precisely why it is recommended to have information available to those participating in the risk assessment at the appropriate time and in the appropriate quality.* The implementation of this principle may be facilitated by the establishment of an appropriate knowledge base, in which the previously arising risk events are described in detail. Naturally, this database must be continuously updated and access to it must be ensured.

▶ *Human behaviour and its culture fundamentally influence the quality of risk management implemented at the different levels and areas of the organisations.* In the language of practice it means that the cultural habits of the given organisation must be taken into account when the risk assessment methods and procedures are selected. In connection with this an incentive system is worth establishing to make the parties participating in the assessment interested in fully exploring the risks, to have the analysis and assessment of the risks suitably substantiated and to really implement the risk management actions specified as a result of the risk assessment.

▶ *Risk management must be continuously improved by processing the experiences and by learning.* This principle means that it is not sufficient for the given organisation to establish and operate the risk management system, but it must also continuously develop it by adjusting it to the circumstances and requirements.

Connecting the risk management system and the targets of the organisation

If the listed principles are fulfilled, there is a good chance to build an efficient risk management system. Efficiency, however, significantly depends on how well risk management is integrated into the responsible corporate governance of the organisations including the decision-making activity. This doubtlessly requires the support of the top management, which must be demonstrated appropriately. One form of manifestation of it is the provision of the personnel, technical and financial resources necessary to operate the system.

Pursuant to MSZ ISO 31000:2018 standard efficient risk assessment and management are only possible if the assessment of the risks is tied to organisational targets. In this case only the risks having direct impact on the implementation of the strategic, operative or project targets of the given organisation are explored and managed.

Furthermore, risk assessment and management connected to the targets will facilitate the easier understanding of the contents of different risks. It will also provide the framework of the assessments performed at the different organisational units, which may be especially useful for the definition of risks with outstanding importance and the specification of risk management actions at company level.

Another key yield of risk assessment connected to the targets is that the decision-making process may be supported with it more efficiently, therefore risk assessment and management become inseparable parts of everyday activities.

This may be illustrated with the following example: during strategy creation an organi-

sation specifies different strategic targets, the achievement of which is made possible by the implementation of, for example, different project ideas (actions). As the funds available for their implementation are generally restricted, a decision must be made as to the implementation of which idea would be desired in the given period.

The different ideas may be evaluated by the yield-risk method and ranked based on the result of the evaluation. The result of the ranking may be one of the considerations as to the implementation of which action is supported by the decision-makers. View *Figure 1* for an example.

Classification of risks into types

Several authors have worked on classifying the risks into types (Blaskovics 2014; Verzuh

2008; Santos 2018; Vaidya, 2018). During the classification, however, these authors did not elaborate how the establishment of groups may support efficient decision-making at the different levels. This is the reason why – based on his research – the author recommends the following classification of the risks (Fekete, 2015):

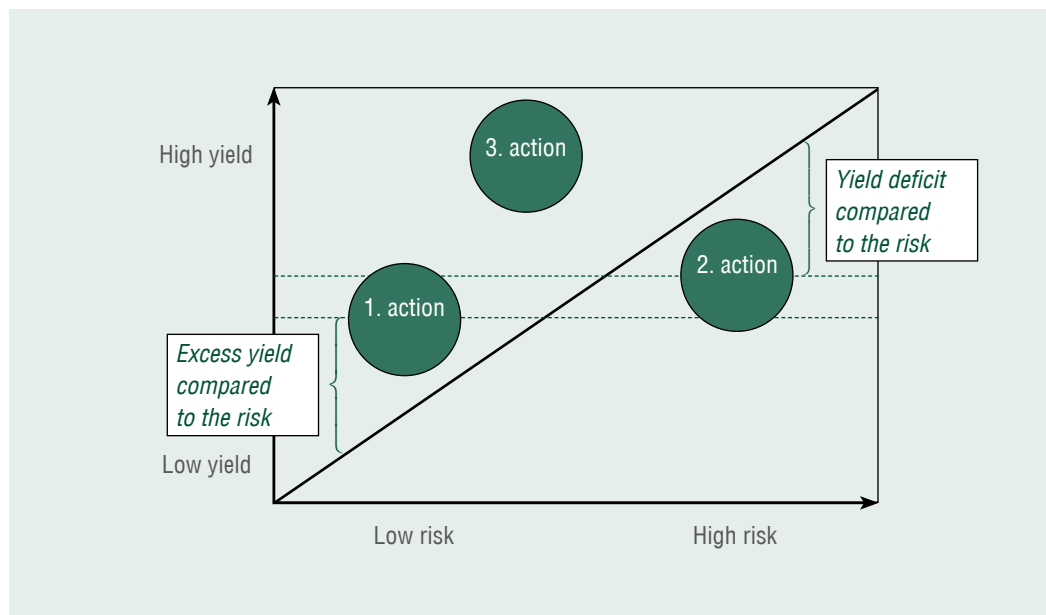
- strategic,
- operational,
- financial,
- project.

Without getting into their detailed presentation, risks are strategic when their impacts appear later (in minimum three-five years). Such risk on the market may be the appearance of a new competitor or the change in the consumers’ habits. The strategic risk must be obviously taken into account during strategy creation.

The next large group is the operational

Figure 1

RESULT OF THE YIELD-RISK EXAMINATION



Source: own edition

risks, the timeframe of which is shorter than that of the strategic risks, typically one year. Operational risk is a generic term including, for example, security risks, compliance risks, but risks arising in connection with the performance of daily routine activities also belong here. An example for the latter is a communication breakdown or failure of the IT system supporting the given activity.

The third large group is financial risks, which also includes different types of risks, including, but not limited to exchange rate risk, interest risk, partner risk and liquidity risk.

The fourth group is project risks, which is in fact the special mixture of the above-listed types, which are, however, worth grouping separately. There could be special risks arising in connection with the preparation and implementation of projects, which must be managed differently from the other three listed types, again including, but not limited to the excavation of archaeological remains or extreme weather conditions, which are typical examples of project risks.

Concept of risk

After the presentation of the principles it is worth briefly explaining the concept of risk.

According to MSZ ISO 31000:2018 referenced above, risk is the effect of uncertainty on achieving goals. What does this mean translated to the language of practice? Uncertainty is due to lack of information. In other words, if every piece of information was available, there would be no uncertainty and risk, either. There is lack of information because risks may arise in the future and the future may not be foreseen precisely.

According to Görög, an important essential feature of solving any problem is the presence of uncertainties in the activity process.

Uncertainty in a sense is the same as lack of information, and uncertainties of different origin often appear in the form of some risk. Risk thus does not exist without uncertainty. Uncertainty means that we do not know the occurrence – or not occurrence – of a given event (its time, place, manner) precisely. Accordingly, uncertainty is ‘neutral’, as we do not know yet if it will have positive or negative consequences for us. As opposed to this, risk generally means the quantifiable negative or positive consequences of uncertainty, while occurrence itself is also uncertain, yet its probability may be described. Consequently, risk may be measured in quantity – the extent of risking –, so it is the product of the probability of negative or positive occurrence and the related loss or gain (Görög, 2008). In order to evaluate the risk, the risk factors becoming the subjects of the evaluation must be defined first.

Other approaches focus on the ‘side effects’. In their case the concept of risk generally refers to an uncertain event, which may have a negative or positive outcome (Hillson, 2002). There is an author, according to whom the level of a given risk may also be specified as the product of the probability of the related events and their size (Hopkin, 2012).

In harmony with MSZ ISO 31000:2018 standard, the definition of risk may be specified as follows (Fekete, 2015).

Risk may be some event, activity or failure of activity, which will take place in the future, and if it occurs, it will influence the reaching of the target positively or negatively.

Elaborating on the concept in more detail we may state that during the identification of risks attempts must be made to direct the specification to the future, to have it interpreted in line with some target. It is also

very important that we generally interpret risks in everyday language with negative outcomes, however the outcome of a risk may also be positive. A good example for this is exchange rate risk, when the exchange rate may also change positively. Risk itself, of course, may also be positive. An example for this is the appearance of much higher than expected demand when a new product/service is introduced. Even positive risks may have negative consequences/outcomes if we are not ready for them in time (for example disappointment due to unsatisfied demand).

Finally, after the brief overview of the standard, the key messages are worth summarising.

▶ The operation of the risk management system will only be efficient if it is supported by the top management of the given organisation. Verbal statements are not sufficient, the necessary human and technical resources as well as methods and procedures based on professional foundation must also be provided.

▶ The integrated nature of the risk management system must be ensured, which, on the one hand, means that it covers every activity of the given organisation, and, on the other hand, in addition to legal compliance, it ensures the efficient support to decisions to be made at strategic, project and operational levels, including the examination of interactions between the different types of risks.

▶ It is important that risk assessment must always be performed in the context of the targets, and attention must be given to identify and evaluate risks meeting the definitions in the relevant academic literature only.

▶ The availability of information in appropriate quality and in time for risk assessment must be ensured, and its result must reflect the opinion of every unit.

▶ It is of key importance that risk management actions specified according to the result of the risk assessment must be implemented – with the considerations of cost efficiency fully taken into account, of course – and the efficiency of the implementation of the action must also be backtested.

GENERAL LIFE CYCLE OF THE ASSESSMENT AND MANAGEMENT OF RISKS

Based on an article published in *Magyar Minőség (Hungarian Quality)* in 2016, the general life cycle of the assessment and management of risks is presented in *Figure 2*. Risk management may be described as the circular cyclic process of the identification, analysis, evaluation and management of risks and the related controlling activity (Cooper, Chapmen, 1987; Chapmen, Ward, 2003; Project Management Institute 6th Edition, 2019).

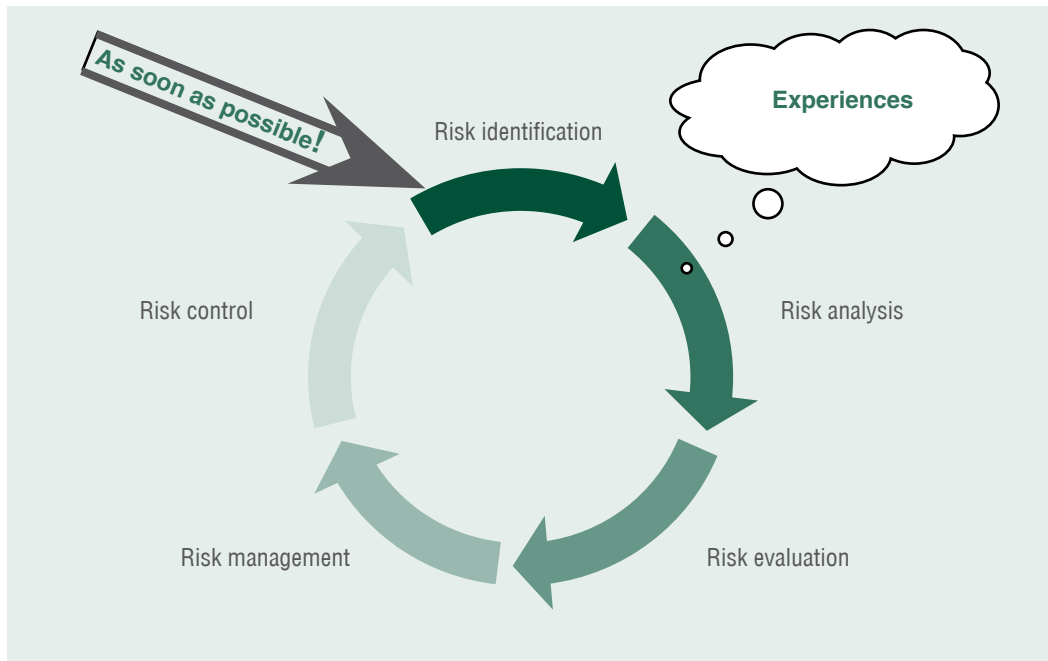
The different steps of risk management described in the Directives follow the specified life cycle. Its application is described in the chapter titled ‘Experiences related to the implementation of the risk management system at a large company’. Following the steps of the life cycle and focusing on another exciting area of risk management, the method usable well in practice to support strategic and project level decisions is presented briefly in the following part of the study.

Risk evaluation process developed by the author to support strategic and project level decisions

There are several methods in the academic literature of risk management (for example PMBOK 6th Edition, 2019; Görög, 2008; Verzuh, 2008) that are suitable for risk

Figure 2

GENERAL LIFE CYCLE OF THE ASSESSMENT AND MANAGEMENT OF RISKS



Source: Fekete, Horváth, Solymos (2016)

evaluation. The majority of them, however, may only be used if there is a sufficient amount of historical information available, which substantiates the application of statistical methods during the evaluation of the risks (Jorion, 1997).

There are different approaches of risk management in the academic literature to analyse the explored risks. (for example PMBOK, 2019; Vysocky, 2014; Richter, McDonough, 2011) These may be categorised into minimum two categories: into the group of qualitative and quantitative methods. Quantitative methods requiring the availability of large amounts of historical data are generally used to support strategic and project level decisions.

The question is raised however, if there is no sufficient historical information available,

why not generate input data necessary for the quantitative evaluation using years of professional experience within the framework of workshops (for scenario analysis, Monte Carlo simulation) to perform reliable risk evaluation.

The author elaborated a previously published method to manage strategic, project and operational risks (Fekete, 2000). This method has been successfully used by him for over 50 different tasks to date. The research performed then, however, did not focus on examining how risk management could efficiently support decision-making in practice. As it was referred to previously, this issue was pushed into the spotlight by the publishing of the ISO 31000:2018 standard. In reaction to this, using his previous research results, the author worked out a flowchart

shown by *Figure 3*. In the following part of the study the relevant steps will be briefly presented – from the focal point of supporting the strategic and project level decision-making process.

Definition of risk sources/events

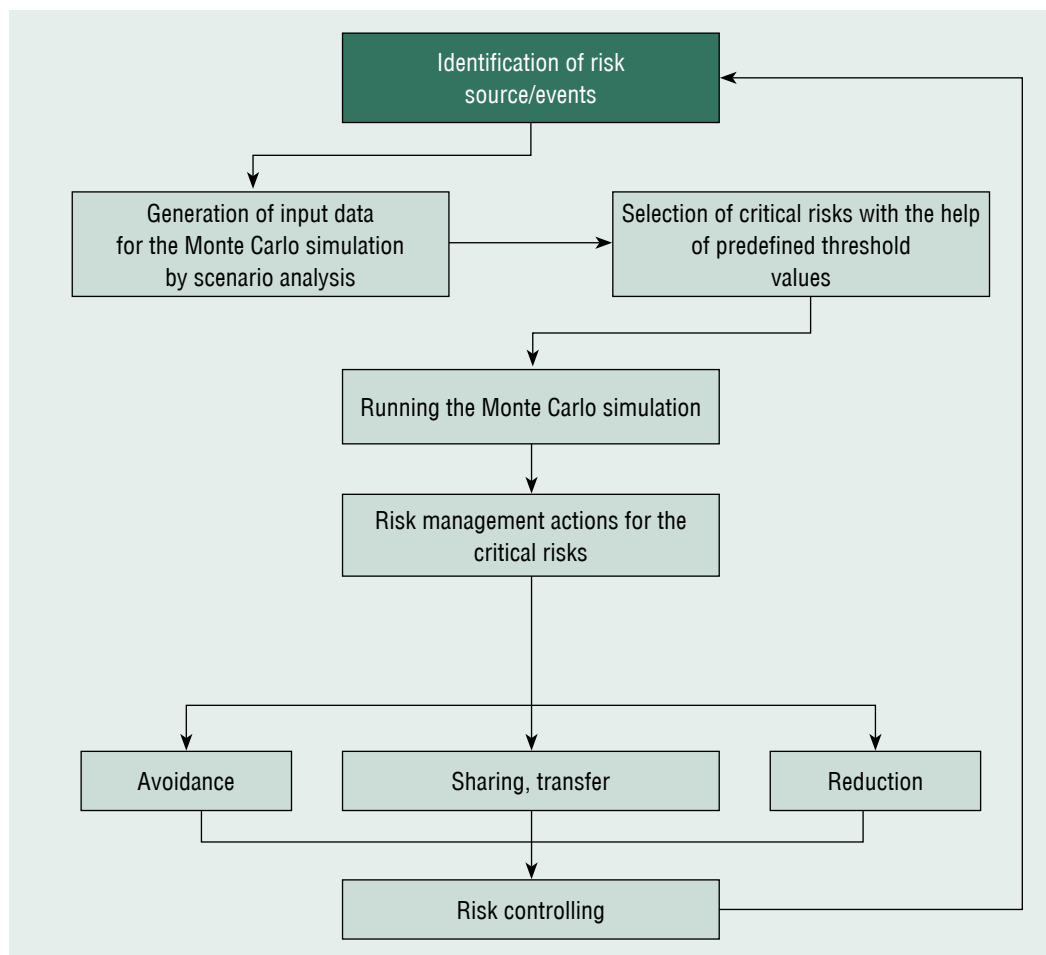
The first task is to define risk sources/events in structured forms, attempting to have complete

definitions, thus increasing the substantiation of decision-making.

This is why the author recommends the use of an ‘intellectual creation technology’ process (such as brainstorming, Papp, 2002) to explore the risk sources/events. The practical performance of the task is within the framework of workshops, which may last from a few hours to a whole day,

Figure 3

FLOWCHART OF RISK MANAGEMENT DEVELOPED BY THE AUTHOR TO SUPPORT DECISIONS AT DIFFERENT LEVELS



Source: own edition

depending on the nature of the task. The achieved result is significantly influenced by the composition of the participants of the workshop. The general rule is that the several years of experience of the experts and their willingness to cooperate in group are important. The courses of the workshops are described in detail by Fekete (2015), and Fekete, Szontágh (2020).

When past data is missing, a database including different potential risk sources/events may come in useful (however, Bakker et al., 2010; Bannermann, 2008; Loosmere et al., 2006; Ohtaka, Fukuzawa, 2010). Such databases are available in large numbers in the risk management academic literature (see Chow, Cao, 2008; Hartman, Ashari, 2002; Lind, Culler, 2011; Summer, 2000).

Specifying the input data of the Monte Carlo simulation by scenario analysis, running the Monte Carlo scenario based on the input data, selecting the risks to be managed

The next step is the quantification of the probability of occurrence and impacts of the previously identified risk sources/events. From the aspect of supporting the decision-making process, the following part of the study will present how the method elaborated by the author may provide input data for one of the quantitative risk evaluation techniques, the Monte Carlo simulation (Herz, 1964).

EVALUATION OF THE IMPLEMENTATION OF PROJECTS. The first step is to draw up a high-level project schedule suitable for the performance of risk assessment. The schedule must include the different activities, the duration of the activities, logical connections between the different activities, as well as the detailed resource and cost plan (Grey, 1995) together with the target values calculated prior to the risk assessment. As we are going to perform activity-based risk assessment during the

implementation, the duration and the costs of the different project activities will be the independent probability variables during the Monte Carlo simulation.

The next step is the identification of the risk sources/events impacting the duration and the costs of implementation of the different activities of the high-level project plan by using the special risk database developed by the author.

Following the identification of risk sources/events, the next step is their evaluation by scenario analysis and the examination of the interactions between the probability variables (Cleden, 2009; Nakatsu, Iacovou, 2009).

Using scenario analysis data, the probability distribution curve of the duration/costs of different project activities is selected. Distributions capable of describing the nature of identified risks most precisely during the project implementation are the beta, gamma, triangle, lognormal and normal distributions (Evans et al., 1993). After this, the typical parameters of the given distribution (expected value, dispersion) must be calculated by using the results of the scenario analysis.

When every piece of input data is available, the simulation may be run and the length and/or total cost of the critical way of the project may be calculated from the large quantity of random data that was generated from the probability distributions assigned to the duration/cost of the activities. This may be performed with the IT programs available on the market (Grey, 1995). The use of the simulation will increase the chance to complete the project in time and within the budget. *Table 1* and *Figure 4* present one example for this.

It is worth mentioning that the described procedure was used for the implementation of several projects of large budgets. The construction of the new Puskás Arena is an outstanding example.

Table 1

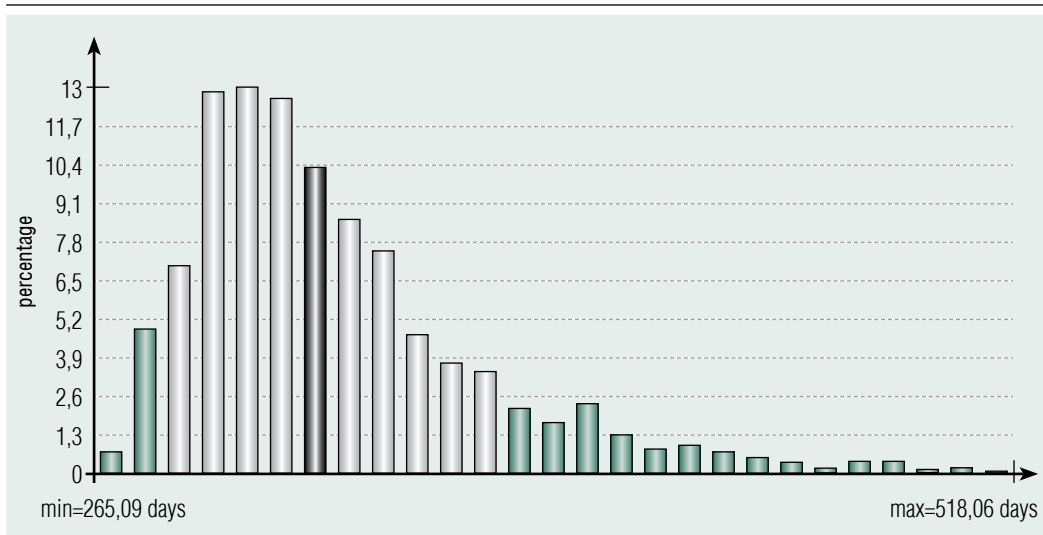
EXAMPLE FOR THE RESULT OF SCENARIO ANALYSIS FOR ONE RISK

SCENARIO ANALYSIS			
Risk factor: Explosive ordnances and military technology artefacts are found while constructing the foundation			
Scenario	Description	Probability (%)	Impact
Scenario 1	There is no such finding, or if there is, the construction of the foundation will not suffer a delay compared to the plan.	98	0 days
Scenario 2	Explosive ordnances and military technology artefacts are found, their examination and preparation for disposal may take a few days.	1	3 days
Scenario 3	Explosive ordnances and military technology artefacts are found, and they explode during the construction of the foundation. The necessary investigation and the repair of the damage may take longer time.	1	10 days
Critical?	Yes.		
Risk management action	Elaboration of a detailed action plan concerning the actions to be taken if explosive ordnances and military technology artefacts are discovered during the construction of the foundation.		
Responsibility	General contractor - project manager		
Deadline	2013. 04. 06.		
Cost	600 000 Ft		

Source: own edition

Figure 4

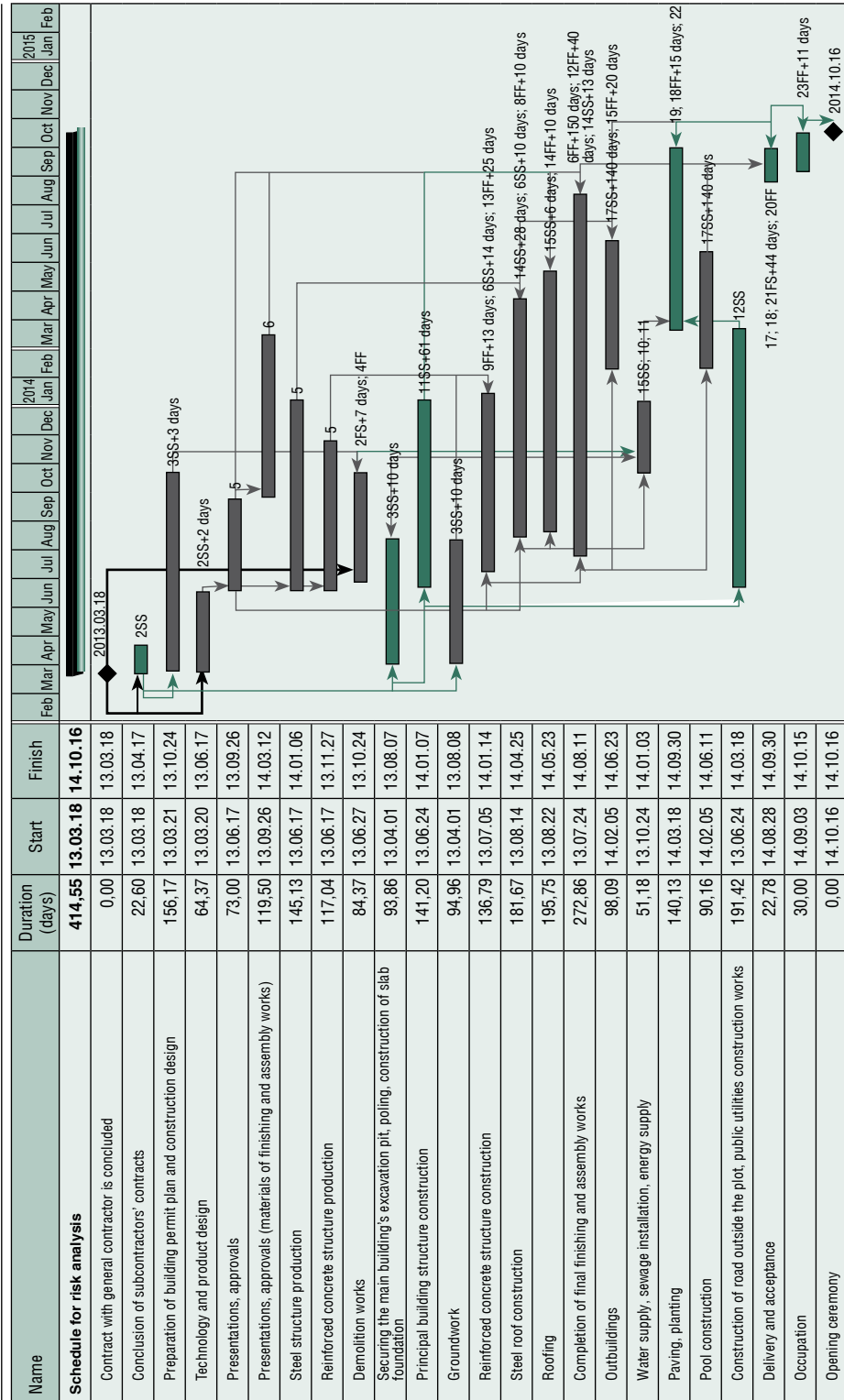
RESULT OF THE MONTE CARLO SIMULATION FOR THE LEAD TIME



Source: own edition

Figure 5

SCHEDULE OF A PROJECT AFTER THE PERFORMANCE OF THE RISK ASSESSMENT



Source: own edition

Figure 5 summarises the schedule of one project after the performance of the risk assessment.

Critical reflections regarding the practical use of the risk assessment methods

At the end of this chapter it is worth summarising what led to the recognition that it was worth elaborating a new approach to support risk-based decision-making.

Before doing so, it is worth stating that techniques already known from the academic literature were used in a new context system.

► Risk management is becoming increasingly important in Hungary today. However, a lot of people still think that anybody may perform the exploration and evaluation of risks without any special preliminary training.

► The other important finding is that in our country we still do not have the culture of integrating the result of risk assessment into the decision-making process at the different levels. The result of the risk assessment appears more as an independent document, the result of which is generally not considered during decision-making.

► It is also an important finding that those performing risk assessment pay little attention to the fact that there is no need to manage every risk. Risk management action is generally defined for every explored risk.

Having recognised all the above points, the author began the detailed research of the academic literature of risk management. Although large volumes of – primarily foreign (American) academic literature – were found, their common characteristic is that they do not elaborate on the reliable way of evaluating risks if there is no past information or if it is not sufficient. One further finding is that the method of

integrating the result of risk assessment into the decision-making processes at different levels is emphasised less.

The essence of the new approach – in the interest of supporting efficient decision-making – may be summarised as follows. !

► In order to have a complete list of risks, even if past data is missing, risks should be explored within the framework of workshops. In the interest of efficient work a preliminary list must be compiled, which will be finalised and extended during the workshop. The preliminary definition of the rules of the workshop and the use of a moderator will also improve efficiency.

► A special procedure was elaborated for the lack or insufficiency of past data, which facilitated the generation of input data necessary to run the Monte Carlo simulation reliably with the help of scenario analysis.

► Finally, a proposal was elaborated for the classification of risks into types to ensure efficient decision-making, which, at the same time, is one of the pillars of setting up the risk management system.

EXPERIENCES RELATED TO THE IMPLEMENTATION OF THE RISK MANAGEMENT SYSTEM AT A LARGE COMPANY

Having taken the principles specified in the directives into account the study presents the experiences related to the implementation of the risk management system with the example of a large company.

The previous chapters of the article presented in detail how the risk management system was to be established based on the different relevant documents (for example standards and the Directives). According to a Hungarian proverb, however, the proof of the pudding is in the eating. The author therefore

visited a large company in Hungary, which had begun the establishment of the system earlier. He was curious to hear the experiences gained by the large company from the establishment of the system, and to what the interviewee would draw the attention of the organisations planning to establish risk management systems in the near future.

This large company is MVM Paks Atomerőmű Zrt. (MVM Paks Nuclear Power Plant Ltd.), a member of the MVM Group, where *Zoltán Gerzsei*, Head of the Management Support Unit talked about the experiences.

The questions were the following.

① Why do you deem the establishment of the risk management system important at the organisation where you work?

② What steps have you managed to take during the establishment and what steps will still be necessary in the future?

③ Is the established system in compliance with the contents of the Directives?

④ What are the experiences concerning the operation of the system so far?

⑤ What should be pointed out to those planning to establish the risk management system in order to comply with the Directives?

IN CONNECTION WITH THE FIRST QUESTION Zoltán Gerzsei explained that risk-aware operation was deemed part of everyday life because of the nature of his organisation. It is particularly true to the recognition and efficient management of the special operational risk, nuclear risks resulting from electric power generation. The strict security provisions specified pursuant to international requirements include the risk assessment and management related requirements and the different steps of the process. Compliance with them is regularly checked by both the competent international and Hungarian organisations. Compliance with these

provisions is important for the power plant, and this may be ensured – among others – by operating the risk management system.

Another key area of risk management used by the power plant is the management of financial risks. Among them the procurement of nuclear fuel is an outstanding risk, as it is procured from abroad by which the company is exposed to a significant exchange rate risk.

In addition to these, the company also recognised that in order to achieve its strategic targets, it was also necessary to explore and efficiently manage operational risks other than nuclear risk, as it is also detailed by the Directives. These areas are the following:

- establishment of an operational risk management system covering every process of the company in the following areas,
 - exploration and management of risks influencing the performance of process indicators resulting from strategic targets,
 - exploration and management of IT and information security risks,
 - business continuity planning.

In the listed areas – also specified by the Directives – work has been performed to date, which, however, has been significantly hindered by the Covid-19 pandemic. When answering the remaining questions, the interviewee focused on the listed risks only.

ANSWERING THE SECOND QUESTION he said that – as member of the MVM Group – MVM Paks Atomerőmű Zrt. had performed the exploration and management of risks pursuant to the group directions.

It is a challenge to adjust the contents of the group directions to the features of the power plant. The company launched more than one project to perform this task, which have already had multiple results, including but not limited to the following ones.

▶ Mapping the company processes, allocating process indicators resulting from the strategic targets to the different processes.

▶ Elaborating risk assessment and management methodology, giving company-level directions to the different areas based on it.

▶ Implementing pilot assessments.

▶ Discussing the experiences of the pilot assessments, elaborating recommendations for the company-level implementation.

During the implementation of the projects the Directives related to the establishment of the internal control system were issued. The staff of the nuclear power plant carefully read the Directives and came to the conclusion that their previously achieved results were largely in harmony with the contents of the Directives, therefore fundamental remodelling was not necessary, but fine-tuning was.

Particular attention was given to the operation of the function supporting compliance with the Directives and already implemented at our company.

The set-up of the control environment and the related risk management system as well as the issue of the related regulations have been basically performed already pursuant to above.

The following tasks are part of fine-tuning:

- drawing up a control strategy and, related to this, the establishment and operation of the control elements, which must be integrated into the already established risk assessment and risk management system,
- elaborating a formal methodology for the evaluation of the internal controls,
- setting up the information and communication system as well as the monitoring system, the foundation of which was established by the already implemented risk management system.

ANSWERING THE FOURTH QUESTION Zoltán Gerzsei said that the colleagues participating in the pilot assessment had approved the steps

already taken concerning the establishment of the risk management system.

The elaborated procedure is clear to them and it fundamentally helps risk-aware thinking. It is important because attempts were made to explore and evaluate the risks already prior to the issue of the Directives. These, however, were stand-alone solutions and did not really allow us to take the interactions between the different risk types into account, to examine the impact made on the implementation of the strategic targets of the power plant during the evaluation of the risks.

It is, however, also important to emphasise that risk assessments have so far been performed for a few selected processes only. It is necessary to expand the assessments to cover every process of the company, to exploit the synergies arising in connection with the assessment of business continuity, IT and information security risks. Currently unknown problems and difficulties may arise during the performance of this work, the solution of which will necessitate the performance of further amendments, fine-tuning.

ANSWERING THE FIFTH QUESTION the interviewee emphasised that based on the contents of the Directives the basis of establishing the control environment was the existence of the processes at the different organisations. This is why the first key task of every organisation wishing to comply with the contents of the Directives is to map and document the processes if the organisation does not have formal processes yet. This is followed by the matching of the established processes and strategic targets, based on which the allocation of the process indicators measuring the reaching of the given strategic target is performed. This is a huge work in the given case. It must, however, be also emphasised that this work is worth performing for other reasons, too, not only to comply with the recently issued Directives.

Pursuant to what is included in the Directives, the risk management system is set up, within which the risk assessment and management methodology is elaborated after the establishment of the processes. The Directives include the principles, which are worth considering during the work. Every single organisation, however, has its own features, which necessitate the customisation of these principles. In nuclear power plants, for example, the system to be set up must comply with international nuclear energy regulations, group-level regulations and the Directives at the same time. In the given case it is worth involving external experts to perform this task.

However, an elaborated methodology not verified by experiences regarding its application in practice is worth nothing. This is why it is absolutely necessary to test the elaborated methodology in some selected processes in the first step, to perform fine-tuning based on the experiences and to finalise the methodology on this basis.

The following key task is the co-ordination of the methodologies elaborated for the assessment and management of the risks and the evaluation of the controls. This fundamentally means that on the basis of the result of the risk management, we can select the risks that definitely need to be managed. These may be new measures (actions) or existing controls (routine measures). In the course of evaluating the risks, the two types must be distinguished and the monitoring of the implementation of the new measures, the backtest of their efficiency must be set up. Based on its result it is possible that a new risk management action becomes a routine measure, internal control later.

Appropriate informing of the decision-makers of the result of the risk assessments is also important. This is the reason why a reporting and monitoring system must be set

up, based on which the decision-makers will receive a realistic picture of the risk exposure of the organisation under their management, the list of risks to be managed, the actions to be implemented and the efficiency of the internal controls. The aim is to make the necessary decisions based on the report and to establish the culture of risk-based decision-making.

All these tasks may be implemented efficiently if appropriate software support linked to the corporate/organisational management systems via interface is available for the performance of risk assessment and management. Appropriate software support also contributes to the setting of the risk database, which may also serve later as a knowledge database.

Last but not least, an established system may only be successful if the concerned colleagues are willing to use it. This is why the involvement of key staff members in the early stage of the process has key importance, providing the opportunity to consider and use their opinion related to the system to be set up. When the system is set up, it is recommended to widely communicate the completion in the form of for example the weekly newsletter or other campaign. This is how the entire organisation will regard the set up system as its own, will use it willingly, thus establishing risk-aware organisational culture and increasing the security.

Factors supporting and hindering the implementation of the risk management system

The author is participating in several projects related to the establishment and operation of the risk management system at different organisations – at large companies particularly.

Based on the conclusions to be drawn from the above interview and using his own experiences, the author summarises the factors supporting and hindering the implementation of the risk management system.

The factors supporting the implementation of the system are the following.

■ Attention must be continuously called to this: the first and outstanding factor is the support of the top management. It must be emphasised repeatedly that this support must cover more than just communication. The necessary human and technical resources must be provided together with a professional procedure for the implementation. It may help greatly if the top managers show a good example in the exploration and management of the risks.

■ In connection with the previous point, the requirements of the owner concerning the establishment of the system, including the advantages of the system's implementation for the employees, must also be emphasised clearly.

■ Implementation may be significantly facilitated by the close cooperation of compliance, internal audit and integrated risk management. This partly concerns the very precise definition of the tasks of the three areas as well as the clear specification of the connection points. This cooperation may only be successful if it is set up among three equal parties and coordinated appropriately by the top management.

■ Furthermore, it is important to mention that the established system must be really integrated. It means that focusing on the exploration, evaluation and management of the compliance risks only is not sufficient, the system must cover the examination of every type of risk having regard also to the potential interactions.

■ It may help the implementation significantly if a procedure clear to everyone and

a methodology facilitating its implementation and easy to use in practice are elaborated.

■ Easy learning of the contents of the methodology description by the persons performing the risk assessment and management must be ensured via examples of cases customised for the given organisation, if possible.

■ No system implementation may be efficient if it is not supported by the staff affected by the process. This is why at the beginning of the system implementation the key staff providing continuous control by giving their opinion, comments, advice, feedback must be selected in order to establish a system really customised for the given organisation supporting the achievement of the targets specified by the organisation.

■ Another supporting factor may be the implementation of a motivation system covering every manager and subordinate staff member participating in the establishment and operation of the risk management system, guaranteeing the successful implementation and operation at the given organisations. One key element of the motivation system is naturally the bonus payment, which is for example tied to the achievement of the targets specified by the given organisation. Motivation, however, may not be limited to this only. It may help significantly if the staff is given the opportunity to participate in trainings related to the topic. Another possibility is to ensure participation at foreign and Hungarian conferences, which is at the same time an excellent opportunity for the participants to do networking.

■ The provision of IT tools to facilitate the operation of the risk management system may also be mentioned among the supporting factors. Note must be taken of the fact that the use of MS Office (Excel, for example) is not sufficient for the performance of the task. If the target is indeed the establishment of

an efficient risk management system, several IT tools may be necessary. There are targeted software tools on the market (for example @Risk, Szigma Integrisk), it is worth selecting one of them with the precise requirements of the given organisation taken into account. It must also be emphasised, however, that none of the IT tools may be magic tools; they may not replace human knowledge and experience.

The factors hindering the implementation of the system are the following.

■ Based on the experiences of the author, the conclusion may be drawn that the added value represented by the implementation of a formalised risk management procedure is not clear, either, for the managers or the subordinates. Many people are convinced that they know the potential risks even without the use of a formalised procedure, and if these risks occur, they will find a way to manage it, therefore it is not necessary to provide serious human and technical resources to perform this task.

■ There are only a few managers who are aware of the fact that the result of risk assessment may directly be built in the decision-making process, and – even if there is formal risk assessment – its result is less considered during decision-making.

■ Another factor worth mentioning among the hindering factors is that many people consider risk management an administrative task, which must be performed due to some provision. In connection with this the negative risks, for example the exploration of risks concerning legal compliance, reputation, security, fraud are shifted to the foreground. These activities include the production of business continuity and disaster recovery plans, which often end up at the bottom of the drawer. These are doubtlessly important areas, however, in the meantime there is no attention and energy for the exploration, evaluation

and management of risks that may directly influence the achievement of the strategic targets of the given organisation positively or negatively. The opinion of the author is that in the long run only organisations exploring, assessing and managing these risks – where the result becomes an integrated part of the decision-making process – will be able to operate successfully.

■ Another hindering factor is that currently there is no higher education training in Hungary, the expressed purpose of which is the training of risk managers. It means that anybody may work in the exploration, assessment and management of risks, which does not necessarily guarantee its professional performance and the possibility of using the result of the risk assessment in effect.

■ Although there are more and more academic books, articles and other publications in Hungarian language, these generally stay at theoretical level. Only a few of them provide professionals with particular methods that are easy to use in practice, or present success stories that serve as positive examples and provide the necessary motivation to perform the risk management activity in higher quality.

■ The number of companies offering risk management advice to potential customers in good professional quality is also low in Hungary. Furthermore, there is no classification criteria system to identify incompetent organisations on the market. Some thought should be given to the establishment and implementation of an objective classification system, if possible. This would result in the fact that companies meeting these criteria would offer authentically high quality services, which may indirectly contribute to the operation of more and more successful companies and institutions in our country.

■ Another hindering factor is that the number of IT tools to be used by the potential

users to perform professional risk assessment, to monitor the implementation of risk management actions and to backtest their efficiency is limited in Hungary. The offer must definitely be increased and the existing tools must be popularised.

Finally, another hindering factor may be the readiness and willingness of Hungarian organisations to require risk assessment and risk management performed at a professionally higher level according to the approach presented in the present study, too.

In connection with this, it is definitely worth considering the establishment of professional forums that would be suitable for the presentation of best practices and for the risk management experts to share their experiences.

By presenting the good practices, every decision-maker must be encouraged to view risk management not as an administrative task, but as an opportunity to receive help for successfully performing the work in the long run. This may be the real added value of risk management.

REFERENCES

BANNERMAN, P. L. (2008). Risk and Risk Management in Software Projects: A Reassessment. *The Journal of Systems and Software*, 81(12), pp. 2118-2133

BLASKOVICS, B. (2014). Az ICT-szektorban működő projektvezetők személyes jellemzőinek hatása a projektsiker alakulására. [Impact of the personal characteristics of projects managers in the ICT sector on project success.] Corvinus University of Budapest

CHAPMAN, C., WARD, S. (2003). *Project Risk Management Processes, Techniques and Insight*. 2nd Edition, John Wiley and Sons Inc.

CHOW, T., CAO, D.B. (2008). A Survey Study of Critical Success Factors in Agile Software Projects. *Journal of Systems and Software*, 81(6) pp. 961-971

CLEDEN, D. (2009). *Managing Project Uncertainty*. Gower Publishing Limited, England, pp. 80-83

COOPER, D. F., CHAPMAN, C. B. (1987). *Risk Analysis for Large Projects: Models, Methods and Cases*. John Wiley and Sons Inc.

DE BAKKER, K., BOONSTRA, A., WORTMANN, H. (2010). Does Risk Management Contribute to IT Project Success? A Meta-Analysis of Empirical Evidence. *International Journal of Project Management*, 28(5) pp. 493-503

EVANS, M., et al. (1993). *Statistical Distributions*. Second Edition, John Wiley & Sons Inc.

FEKETE, I. (2000). Kockázatelemzés szerepe a beruházások pénzáramlásának meghatározásában. [The role of risk analysis in defining the cash flow of investment projects.] PhD Dissertation, Budapest University of Technology and Economics, Budapest

FEKETE, I. (2015). Integrált kockázatmenedzsment a gyakorlatban. [Integrated risk management in practice.] *Vezetéstudomány [Management science]*, January 2015, pp. 33-46

FEKETE, I., SZONTÁGH, P. (2020). Projektek programszintű kockázatmenedzsmentje. [Program-level risk management of projects.] *Vezetéstudomány, [Management science]*, February 2020, pp. 18-27

- GÖRÖG, M. (2008). *Projektvezetés. [Project management.]* Akadémiai Kiadó, [Academic Publisher], Budapest, pp. 137-150
- GREY, S. (1995). *Practical Risk Assessment for Project Management.* John Willey & Sons Ltd., pp. 81-97
- HARTMAN, J., ASHARI, R. A. (2002). Project Management in the Information Systems and Information Technologies Industries. *Project Management Journal*, 3383, pp. 5-15
- HILLSON, D. (2002). Extending the Risk Process to Manage Opportunities. *International Journal of Project Management*, 208(3) pp. 235-240
- HOPKIN, P. (2012). *Fundamentals of Risk Management: Understanding Evaluating and Implementing Effective Risk Management.* 2nd Edition 18. The Institute of Risk Management
- HORVÁTH, Zs., SOLYOSI, I., FEKETE, I. (2016). Gyakorlati tanácsok a kockázatfelmérés és kezelés szervezeti szintű bevezetésére a vonatkozó szabványok alapján. [Practical advice on the organisation-level implementation of risk assessment and management based on the relevant standards.] *Magyar Minőség [Hungarian Quality]*, 25(5), pp. 1-22
- JORION, P. (1997). *Value at Risk The New Benchmark for Controlling Derivatives Risk.* The McGraw-Hill Companies Inc.
- LIND, M. R., CULLER, E. (2011). Information Project Performance: The Impact of Critical Success Factors. *International Journal of Information Technology Project Management*, 2(4), pp. 14-25
- LOOSEMORE, M., RAFTERY, J., REILY, C., HIGGON, D. (2005). *Risk Management in Projects.* Second Edition, Taylor & Francis, pp. 43-65
- NAKATSU, R. T., IACOVOU, C. L. (2009). A Comparative Study of Important Risk Factors Involved in Offshore and Domestic Outstanding of Software Development Projects. *A Two-Panel Delphi Study Information & Management* 46(1) pp. 57-68
- OHTAKA, H., FUKAZAWA, Y. (2010). Managing Risk Symptom: A Method to Identify Major Risks of Serious Problem Project sin SI Environment using Cyclic Causal Model. *Project Management Journal* 41(81), pp. 51-60
- PAPP, O. (2002). Projektmenedzsment a gyakorlatban. [Project management in practice.] LSI Oktatóközpont [LSI Training Centre], Budapest, pp. 198-213
- RICHTER, L., McDONOUGH, M. (2011). brighthubpm.com. Source: top ten project risk management books: <https://www.brighthubpm.com/risk-management/91928-top-ten-project-riskmanagement-books/>, Date of download: 5 October 2018
- SANTOS, D. M. (2018). top-10-best-project-management-books-to-keep-within-reach. Source: project-management.com: <https://projectmanagement.com/top-10-best-project-management-books-to-keep-within-reach>, Date of download: 5 October 2018
- SUMMER, M. (2000). Risk Factors in Enterprise-wide/ERP Projects. *Journal of Information technology*, 15, pp. 317-327
- VAIDYA, D. (2018). wallstreetmojo.com. Source: Top 9 Best Project Management Books of All Times, <https://www.wallstreetmojo.com/projectmanagement-books>, Date of download: 6 October 2018
- VERZUH, E. (2008). *The Fast Forward Mba in Project Management* (Third edition). New Jersey: John Wiley & Sons, Inc.

WYSOCKY, K. (2014). *Effective Project Management. Traditional, Agile, Extreme* (Seventh edition). Indianapolis: John Wiley & Sons, Inc.

MSZ ISO 31000 (2018). Risk Management - Principles and Guidelines by the International Organization for Standardization.

PMBOK 6TH Edition, (2019). A Guide to the Project Management Body of Knowledge, Fourth Edition Project Management Institute.