AN INTEGRATED RISK MANAGEMENT SYSTEM AS AN EFFECTIVE TOOL FOR DEALING WITH A PANDEMIC SITUATION

Renata Nováková*, Viera Horváthová, Andrea Vadkertiová

Institute of Management, University Ss Cyril and Methodius in Trnava, Nám. J. Herdu 2, Trnava 91701, Slovakia

Abstract

The pandemic situation caught us off guard. Although many organizations have strategic crisis management plans and ISO 31000-certified risk management systems, many SMEs are unable to anticipate risks and, worse, do not know the basic management methods and tools that classify such risks, and create the conditions for their mitigation. The subject of our paper will be to define and classify risks and relationships in risk management as an integrated system.

Keywords: *risk management, ISO standards, effective tools, integrated risk management system*

1. INTRODUCTION

The concept of risk has its basis in history. In the older literature, it was explained as exposure to adverse circumstances, or dare to do something that may have an uncertain outcome and be related to a threat. Recently, the concept of risk often inflected in all sorts of contexts such. For example: risk countries, risk of virus infection, risk of job loss, risk of damage, risk of loss of health, risk associated with insufficient financial assistance, risk associated with travel, etc. This way we could go even further. The reason is very prosaic. The concept of risk is very topical, as it is linked to the current pandemic situation, which has affected our personal and working lives as a "flash from the clear sky". What is striking, however, is that many, especially large organizations, have developed a relatively detailed risk management system, which is usually part of crisis manuals. Despite many indications from the past, this type of risk was approached quite generally and the context was not defined in advance. However, before we focus on an integrated risk management system as a possible effective tool for dealing with any non-standard situation, we need to get a little closer to the types of risks and their basic distributions.

2. TYPES OF RISKS AND THEIR CHARACTERISTICS

In practice, we most often encounter economic risk in the business environment. However, in addition to this, there are other risks such as:

- Political and territorial

- Economic - macroeconomic and microeconomic (market, inflation, exchange rate, credit, trade, payment .....)

- Security

- Legal and risks associated with liability for damage

- Specific, which are related to e.g. with the management system, financial market, innovation risks, sales risks, etc.)

The most important risk characteristics are:

• Probability of risk - the probability that a risk will occur

• Level of risk

• Impacts of risk - the consequences that will occur if a risk situation occurs

• Predictability of risk - the chance that the risk can be identified and predicted in advance

• The degree of risk affectability

- Influenceable
- Partially affected
- Unaffected

• Relationship to the organization

- Internal risks - these types of risks can be influenced and managed by the entity, they manifest themselves within the organization
- External risks - these types of risks cannot be directly influenced by the entity, these are environmental factors

• Order of action - origin and removability

- Primary
- Secondary - these types of risks arise when eliminating primary risks
- Residual (residual, residual) - this type of risk remains after the elimination of the risk, it is a risk that the entity is willing to bear

• The size of the risk

- Small
- Medium
- Great

• Acceptance rate (acceptability, tolerability)

- Necessary (necessary)
- Bearable (acceptable)
- Unsustainable (unacceptable)

• Probability of occurrence and effect

- Unlikely
- Unlikely
- Probable
- Very likely
- Almost certain

• Scope of operation

- Systematic - this type of risk applies to all business entities
- Unsystematic - this type of risk applies only to a certain branch of business (www.managementmania.com/sk/rizika)

Classification of types of risks in the organization:

• Operational risks

- Technical (technological) risks
- Production risks

• Information risks

• Economic and financial risks

- Credit risks
- Insolvency risk
- Investment risks - estimating the profitability and reliability of an investment
- Insurance risks - an estimate of the size of the risk and the probability of an insured event
- Currency risks - risks arising from changes in exchange rates in international trade

• Market risks

• Marketing risks

• Social risks

• Business risks

• Legislative risks

• Logistic risks

• Political risks

• Business risks

• Project risks

• Social risks

• Environmental risks

• Natural and natural hazards

In the literature we can find a number of more or less detailed breakdowns of risks and their characteristics. However, the subject of our interest will be to characterize risk management in more detail. An important part of risk management is risk reduction using risk prevention methods and techniques. Their task is to eliminate or detect in time the factors that increase the risks. In an environment where there is a high degree of uncertainty, risks are more likely to arise. Risk analysis very often works with variables that cannot be accurately measured, and in many cases their more accurate identification is left to the qualified judgment of a specialist who has sufficient experience and knowledge. Very often, a verbal form is used to express the extent, respectively. Severity of risk such as small, medium, large, or a scale from 1 to 10 is used. (Smejkal,V., Rais, K.: Řízení rizik ve firmách a jiných organizacích, Grada Publishing 2010)

3. PROBABILITY OF RISK OCCURRENCE

There is another very important concept associated with risk, and that is the probability of occurrence. If the risk is defined as the possibility of an unfavorable deviation from the desired result that we expected or hoped for, the degree of risk is measured by the probability of this unfavorable deviation. (Likeš, J., Machek, J.: Probability Number, SNTL, Prague, 1983)

Following the above fact, we must deal with the so-called the expected (expected) value of the loss. This can be graphically represented as follows:

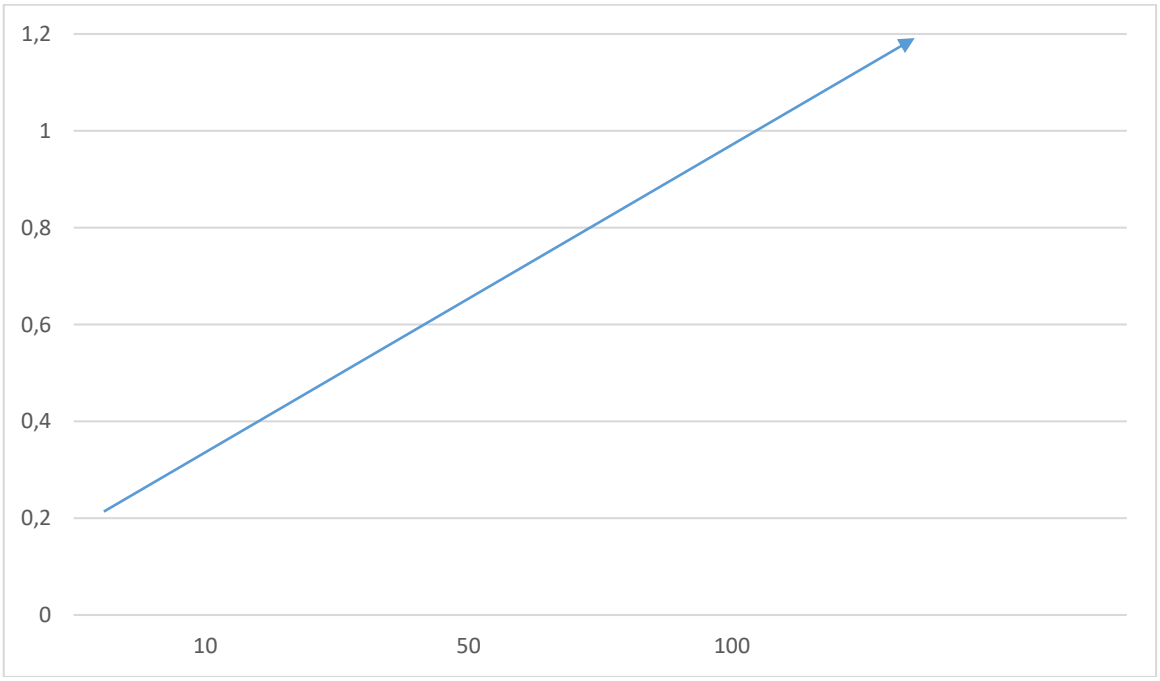

Fig. 1. Estimated amount of loss

Likeš, J., Machek, J.: Probability Number, SNTL, Prague, 1982

4. RESULTS

The calculation of possible loss is expressed by the relation:

Possible loss = risk x size of loss

The size of the assumed loss Z (t) in the time interval <0, T0>:

$$Z(t) = \int_0^T r(t) \,.\, v(t) \,.\, dt$$

Where:

r(t)..... is the function of risk over time expressed by the probability of the interval$< 0,1 >$

v(t)..... is a function of loss in time (in practice this function is a step, it takes values 0 or 1)

Z (t) ..... it is the size of the expected loss in the time interval <0, T0>

(Smejkal,V., Rais, K.: Řízení rizik ve firmácha a jiných organizacích,Grada Publishing, 2010

5. DISCUSSION - RISK ANALYSIS METHODS

Risk analysis methods can be divided into:

Qualitative methods - are based on the description of the severity of the potential impact on the probability that the situation will occur. The level of risk is in most cases determined by a qualified estimate. It can be said that qualitative methods are simpler and faster, but they are also more subjective. There is a lack of a clear financial statement, which makes it more difficult to control cost-effectivenes

Quantitative methods - are based on a mathematical calculation of risk from the frequency of the threat and its impact, which is most often expressed financially. The most common risk is expressed in the form of annualized loss expectancy (ALE). Quantitative methods are more exact. Their implementation requires more effort and time, but this is important, they provide a financial expression of the risks and the quality of the results is closely linked to the relevant data.

Combined methods - based on numerical data. Thanks to the qualitative evaluation, they are closer to reality than the assumptions on which the quantitative methods are based. However, they may be affected by the scale that is used in a particular case.

The most commonly used methods for risk analysis are as follows:

a) Method of targeted interviews (Delphi method) - this is the management of contacts between the experts of the evaluation group and the relevant representatives of the evaluated entity. A set of questions is used here, which is discussed in special-purpose interviews. The questions are made up of a fixed and a variable form. Respondents are asked individually, so it is guaranteed that they cannot influence each other in their answers. The advantage of this method is less demands on resource consumption, time, taking into account the specifics of the system under assessment and under. The Delphi method is suitable for risk analysis because it determines what can happen and under what conditions. (Catalog of control methods, INORGA, Ostrava, 1982)

b) Quantitative methods for computer processing - these methods are used mainly in the field of security of organizations and their information systems - it is e.g. on CRAMM, COBRA, MELISA methodologies. The best known is probably the CRAMM (CCTA Risk Analysis and Management Methodology) method, which was originally developed for the needs of the UK government, but is currently used for cases of compliance with ISO 13 335 ISO / IEC 13335-1: 2004 - Information technology - Security techniques - Management of information and communications technology security - Part 1: Concepts and models for information and communications technology security management and the international standard ISO 27 000. CRAMM depends on the results of structured interviews with user experts

c) Other methodologies for quantitative risk analysis:

@RISK methodology - used for risk analysis of Monte Carlo simulation methods. The whole issue is processed in the form of tables. The decisive factor of this method is the design of the model, which defines the situation in the form of a table. It is essentially a quantitative method that determines the probability distribution of threats and risks.

RiskPAC methodology - used to automate questionnaire approaches. RiskPAC makes it possible to solve the processed method of questionnaire surveys in the form of automated evaluation. Risks are automatically determined here, the whole result is based on artificial intelligence.

RiskWatch - this is a software product that will provide a methodological file for detection, simulation and subsequent change of parameters of individual system risks. The method is based on the creation of a model that is based on the obtained data or on the Monte Carlo simulation method. It is a structured set of questions according to security areas.

ISO 31 000 standard and integrated risk management system

Since 2009, the ISO 31000 group of standards has been a guide for risk management. These included the following standards:

ISO 31000: 2009 - Risk management - Principles and guidelines, in the Slovak Republic taken over as STN ISO 31000: 2011 Risk management, principles and guidance - codified by the International Organization for Standardization, which provides general guidance for designing, implementing and maintaining risk management processes in the organization

• ISO / IEC 31010: 2009 - Risk management - Risk assessment techniques, in the Slovak Republic taken over as STN EN 31010: 2011 Risk management - Risk assessment techniques - codified by the International Organization for Standardization and the International Electrotechnical Commission, which supports the ISO 31000 standard and provides information, concerning the selection and use of risk assessment techniques. It aims to promote mutual understanding and a consistent and coherent approach to the description of activities related to risk management and the use of common terminology for risk management in the processes and structures dealing with risk management. It states the sequence of risk management (identification of risk and causes of its occurrence, determination of consequences

when the risk is realized, determination of the probability of recurrence of risk, identification of factors that reduce the consequences or probability of risk management processes in the organization)

ISO 31000: 2018 Risk Management - Guidance - replaces ISO 31000: 2009 Risk Management - Principles and Guidance, issued in February 2018

In older literary sources it is still possible to trace:

• ISO / IEC Guide 73: 2009 - Risk Management - Vocabulary – Guidelines for use in standards, in the Slovak Republic as Risk Management - Glossary - Guidelines for use in standards, an international standard that provides terms and definitions for risk management. In addition to these standards, risk management addresses:

• ISO Guide 51: 2006 - Safety aspects - Guidelines for their incorporation into standards.

A Risk Management Standard - IRM / ALARM / AIRMIC 2002 - A risk management standard developed by three major UK risk management organizations - "A combination of probability of an event and its consequences". These standards are or will be used for risk assessment in all standards for management systems adapted to Annex SL (formerly ISO Guide 83), e.g. quality management system, information security management system, business continuity management system, environmental management system, occupational health and safety management system and in other management systems.

Several management systems are certified in organizations and therefore the ambition is to create an integrated risk management system according to the ISO 31000 standard with a focus on the requirements of the ISO 9001: 2015, ISO 14001: 2015 and ISO 45001: 2016 standards. An important prerequisite is the so-called risk-based thinking. The integration of the risk management system is based on the following components of individual normative documents:

ISO 9001: 2015 - Chapter 6 Planning- 6.1. Risk and opportunity management measures

ISO 14001: 2015- Chapter 6 Planning - 6.1. Activities to address risks and opportunities

6.1.1. Generally

6.1.2. Environmental aspects

6.1.3. Mandatory requirements

6.1.4 Activity planning

ISO 45001: 2016 - Chapter 6 Planning - 6.1. Measures to address risks and opportunities

6.1.1 General

6.1.2 Hazard identification and health and safety risk assessment

6.1.3 Determination of applicable legal and other requirements

6.1.4 Planning for action

With an integrated risk management system, it is very important to measure performance using indicators, regularly compare the actual situation with the plan and identify any deviations, periodically review the suitability of the risk management system, policy and plan, report risks, trends in the risk management plan and review the effectiveness of the management system. risks.

6. CONCLUSIONS

The biggest problem of risk management is the question of chance, unexpected events that did not occur in the past at all, or only exceptionally. The author Nassi Nicholas Taleb elaborated the so-called "black swan" theory. These are unexpected phenomena or events that have a very wide impact, are very difficult to predict and completely deny all expectations, respectively. are not based on any previous experience. Despite the fact that we are talking about how the so-called the black swan is unpredictable, so it

becomes explainable and even logical. Many times we may even come across the opinion: "it was to be expected after all ...." Black swans became black swans only due to human unpreparedness. It is a mistake that we take our proven knowledge of the past as definitive and general and valid in all circumstances. However, black swans are the cause of big crashes, but also big opportunities. N.N. Taleb recommends that management systems be built that are resistant to black swans, but at the same time are able to take advantage of the opportunities that may arise due to black swans. It means so much that it is not always possible to predict what may happen. This in many cases, such as even this pandemic COVID-19 situation, we cannot. But we must be vigilant and see things in a broader context. (Taleb, N.N .: The Black Swan. The Impact of the Highly Improbable. Penguin Books Ltd., 2008) probable. Penguin Books Ltd. , 2008)

ACKNOWLEDGMENTS

The publication output follows the project KEGA 012UCM-4/2020 System applications of the foresight process in the new study program Safety Engineering and is part of the research within this project.

REFERENCES

1. Smejkal,V., Rais, K.: Řízení rizik ve firmách a jiných organizacích, Grada Publishing 2010
2. Likeš, J., Machek, J.: Počet pravdepodobnosti, SNTL, Praha, 1983
3. Katalog metód riadenia, INORGA, Ostrava, 1982
4. Taleb,N.N.: The Black Swan. The Impact of the Highly Improbable. Penguin Books Ltd. , 2008
5. Normy ISO 9001,14001,4500, 31000
6. Anderson,D, Sweeney,D., Williams, T.: Statistics for Business and Economics. 8.vyd. South-Western, 2001, ISBN 0324066716
7. Culp,Ch.L.: The Risk Management Process.Business Strategy and Tactics.John Wiley &Sons, 2001, ISBN 047140554X
8. Dembo,R.S., Freeman,A.: The Rules of Risk. A Guide for Investors. John Wiley &Sons USA, 1998, ISBN 0471247367
9. Belan, Ľ.: Bezpečnosť a manažérstvo rizika – 2.časť, ŽU Žilina, 2015
10. www.managementmania.com/sk/rizika