Risk managent in IT

Introduction to risk management

Stanislav Masák, MSc.

masakst@gmail.com

Lesson: personally
class A-162 , 10.00 – 13.00
28.9., 12.10., 26.10., 9.11., 23.11., 7.12.

Seminars: online
MS TEAMS, 10.00-11.30
5.10, 19.10, 2.11, 16.11, 30.11, 14.12.

Risk management

This is an area of management that focuses on risk analysis and mitigation. The goal of risk analysis is the elimination or reduction and, in fact, in its essence, the detection of all potential risks.

What is risk? According to the definition of the Ministry of the Interior of the Czech Republic = The possibility that an event will occur with a certain probability that we consider undesirable from a security point of view. Risk is always derivable and derived from a specific threat. The level of risk, i.e. the probability of harmful consequences resulting from the threat and the vulnerability of the interest, can be assessed on the basis of a so-called risk analysis, which is also based on an assessment of our readiness to face threats.

Glossary:

Risk - a potential event in the future with negative consequences. So the risk may or may not occur. Certain risks are associated with every activity, therefore risks have always been, are and will be present in the operation of every organization. The goal is therefore not to eliminate all risks, but to be aware of them and work with them (i.e. manage them).

Asset - It is anything (tangible or intangible) that can be used to produce positive economic value. Assets represent value of ownership that can be converted into cash.

Risk management – an integral part of every decision in the organization. Continuous activity aimed at reducing the probability of occurrence of risks or reducing their impact. The purpose of risk management is to prevent problems or negative phenomena, i.e. prevent the occurrence of problems and thereby avoid the need for crisis management.

Risk significance – the relative importance of the risk to the organization, which is usually expressed as the product of the probability of the risk and the impact of the risk. (Hereinafter referred to as V).

Glossary:

Risk probability – the degree of probability of a risk event occurring in the future, measured according to prevailing practice on a scale of 1-5 (1 least likely, 5 most likely). (Hereinafter referred to as P).

Risk impact (effect on the organization) – the extent of the negative impact or loss that the organization will incur in the event of a risk event. It can include both direct financial losses or additional costs, as well as impacts of a non-financial 4 nature, e.g. loss of good reputation, reduction in the quality of services for citizens, etc.). According to the prevailing practice, the impact of the risk is again measured on a scale of 1-5 (1 the least negative impact, 5 the greatest negative impact). (Hereinafter referred to as D).

Risk map – result of risk analysis; an overview of the organization's identified risks can be sorted according to their significance in the program, which serves as one of the bases for compiling - these risk maps serve and for the purposes of managing the organization's risks by its management.

Glossary:

Top management of the organization – 1st and 2nd level of organization management, director and deputies, heads of key departments, e.g. economic or financial department, informatics department, legal department

Managers at other levels of management – other managers at lower management levels of the organization.

Risk management is a continuous, recurring set of interconnected activities, the goal of which is to manage potential risks, i.e. to limit the likelihood of their occurrence or reduce their impact on the organization and its goals. The purpose of risk management is to prevent problems or negative phenomena, to avoid crisis management and to prevent the emergence of problems. Risk management consists of several interconnected phases - 4, 5, 6 or 8 are distinguished according to different methodologies. 6 basic phases are most often used, namely:

- risk identification
- risk evaluation
- risk management
- risk analysis
- risk mitigation
- risk monitoring and review

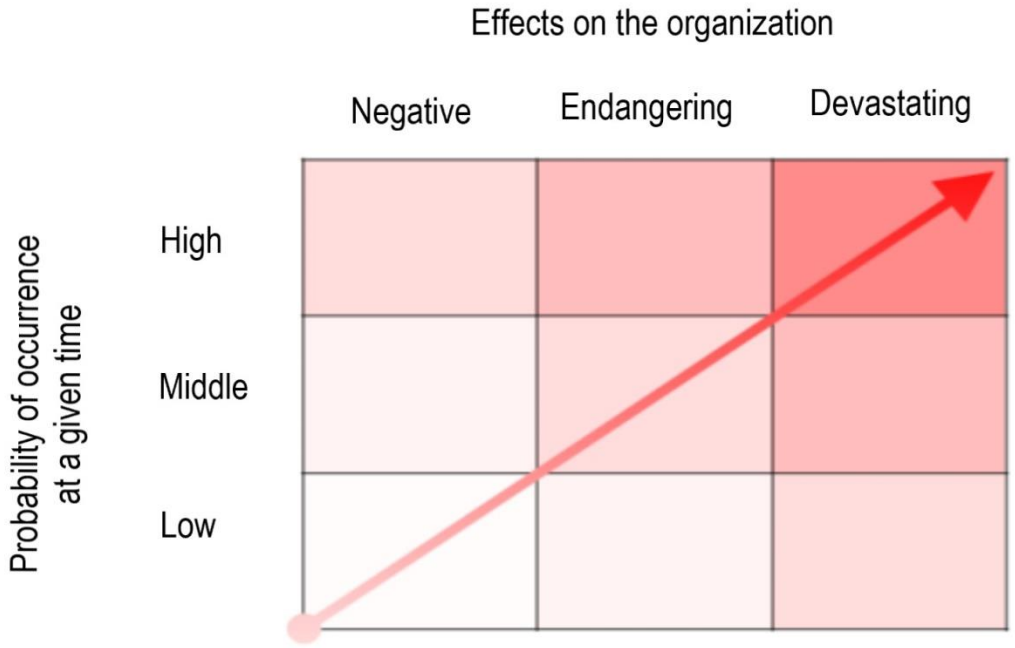
Fundamental to risk management is its analysis. Risk analysis is used to determine the degree of danger (threat) to which the organization is exposed, how vulnerable its assets are to these threats, how likely the threat is to occur (vulnerability) and what impact it may have on the organization. The basic principles of risk management can be summarized in the following statements:

- Every human activity brings certain risks
- Zero risk does not exist

In organizations, responsibility for risk management is distributed throughout management. The highest responsibility naturally rests with the owner, the statutory body and the top management of the company.

In small organisations, responsibility for risk management is concentrated at the level of the statutory body, as it is not efficient to employ a dedicated full-time risk manager. In medium and large organizations, responsibility is distributed among individual managers. Large organizations or organizations doing business in a risky environment (for example, banks, insurance companies, petrochemical and energy industries, aviation industry, transport) have a designated specialist (risk manager). Risk management is almost always linked to the role of the CFO, as the effects of risks (damages) and countermeasures can be expressed financially and have an impact on financial planning.

Winterling crisis matrix - a graphical representation used to interpret the risk map



Risk management models applied in practice

A centralized risk management model

Brief description: The risk management of the organization is in charge of the Risk Management Committee consisting of the top management of the organization. One of the organization's employees (risk manager) is tasked with coordinating activities in the area of risk management across the organization and preparing documents for meetings and decision-making by the Risk Management Committee. Prerequisites An employee who is in charge of coordinating risk management in an organization must have sufficient knowledge, experience, competence and trust on the part of the top management of the organization as well as managers at other levels of management in order to be able to ensure:

- Active and open communication with members of the Risk Management Committee
- Preparation of complete and true documents (in cooperation with senior staff at all levels of management and specialist departments) including the inclusion of negative information and possible impacts related to the given operation, which are relevant for deciding on the next course of action

Risk management models applied in practice

• Submission of these documents to the Risk Management Committee and active participation in their discussion Members of the Risk Management Committee must be willing and able to accept the existence of risks in the operations under their management, not try to marginalize them and continue to work with them, not only individually, but even in front of other members of the top management of the organization.

Advantages:

It allows the organization to emphasize risk management in the form of separate activities aimed at identifying, evaluating, monitoring and reporting significant risks in the organization. When properly implemented, it gives the organization's top management reasonable assurance that key risks are being consistently managed by executives at the appropriate levels of the organization.

Risk management models applied in practice

Disadvantages:

Among the most frequently identified shortcomings of risk management are a tendency towards formalism, understanding the organization's risk map or risk catalog as the goal of activities in the area of risk management, not as a mere tool for active risk management by the organization's management, and excessive emphasis on quantifying the significance of risks, rather than on further work with by them. All these shortcomings are naturally supported by the introduction of a centralized risk management model rather than prevented. It is therefore a model in the environment of non-profit organizations suitable only for those organizations that really operate in a risky environment and where the functioning of the risk management system in the form of separate activities aimed at identifying, evaluating, monitoring and reporting significant risks is therefore key to their successful functioning. In other organizations that operate in a standard environment, where the worst possible negative impact of a bad decision is financial loss, additional costs or possible administrative or legal proceedings, this risk management model is not very effective, and in practice, its disadvantages tend to be more apparent.

Risk management models applied in practice

Decentralized risk management model

Brief description: Risk management is an integral part of every decision made within the organization by its managers. From a certain level of significance of the decision taken, risk management must have its documented form so that an audit trail remains in the organization. The level of significance is determined by the organization itself in its internal regulations and can, or it should be different for different types of operations in different areas (according to the riskiness of operations of a given type in a given area for the organization in general).

Prerequisites for functioning: Managers at all levels of management must understand what risk is and how to work with it, and consciously apply this knowledge in practice when managing the department entrusted to them, always in proportion to the operation they are deciding on.

Risk management models applied in practice

Advantages:

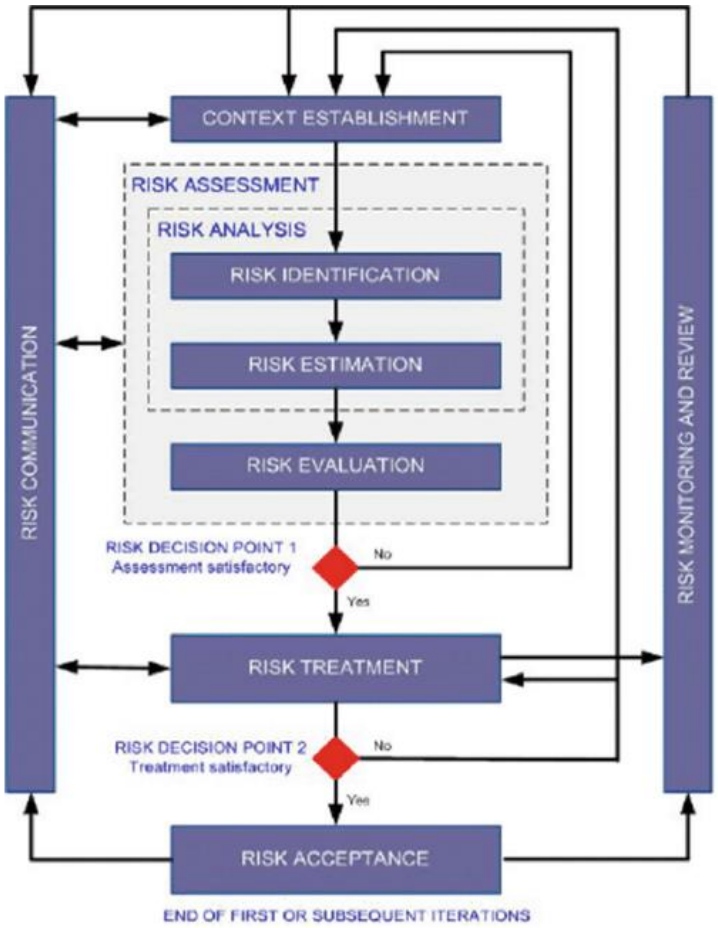
It eliminates most of the disadvantages of a centralized risk management model. It does not assume the existence of a central risk coordinator, from whom it is naturally very difficult to demand such a degree of knowledge, experience and competence in the public administration environment that he would be an equal partner to the top management of the organization in the discussion of risk management.

Disadvantages:

In order to function optimally, it requires the active participation of all senior employees at individual management levels. However, a condition for the good functioning of the decentralized risk management model is not that it be applied perfectly across the entire organizational structure from the very first moment. Somewhere it can work better and somewhere worse, it depends on specific managers. Gradually, it can be unified across the organization in the form of transferring good practice from the departments where it works to the others.

Risk management models applied in practice

Algorithm of possible risk management



ISO 31000 is a family of standards relating to risk management codified by the International Organization for Standardization. ISO 31000:2018 provides principles and generic guidelines on managing risks faced by organizations.

ISO 31000 seeks to provide a universally recognized paradigm for practitioners and companies employing risk management processes to replace the myriad of existing standards, methodologies and paradigms that differed between industries, subject matters and regions. For this purpose, the recommendations provided in ISO 31000 can be customized to any organization and its context.

As of 2020, ISO/TC 262, the committee responsible for this family of standards, has published five standards, while four additional standards are in the proposal/development stages.

Meaning of the standard:

The purpose of the standard is to ensure the influence of business risks with regard to the internal and external environment, and this by appropriate risk management in such a way that the occurrence of risks is reduced with regard to their impact on the organization.

Use / application of the standard:

This standard defines the requirements for a risk management system and is applicable to all types of organizations, it can be used for both service and manufacturing sectors. It is applicable to any type and size of organization.

ISO/IEC 27001 - Information security management

History: The first standard covering information security requirements was BS 7999. The aim of this first standard was to define the requirements for the protection of information in general, i.e. stored not only on electronic media, but also printed or communicated by word or image. Since the development of technology since 2000 has brought IT technologies a dominant role in the field of information, this caused the need to create the ISO 27001 standard in 2006 and subsequently amend it in 2013.

The principle of the norm: The ISO 27001 standard is an internationally valid standard that defines the requirements for an information security management system. The standard specifies information security management requirements, requiring the company to handle all internal information or information shared with its partners or employees in such a way that it is not lost, misused or even just a violation of trust.

The contribution of the standard to the organization

· brings, thanks to the standardization of processes, the efficiency of activities in the classification of risks associated with the loss or misuse of information

· will enable individual companies to gain confidence in sharing information with their business partners

· will reduce the risk of additional costs related to possible unexpected events

ISO 27002 Information security, cybersecurity and privacy protection — Information security controls

Abstract:

This standard provides a reference set of generic information security controls including implementation guidance. This standard is designed to be used by organizations:

a) within the context of an information security management system (ISMS) based on ISO/IEC27001;

b) for implementing information security controls based on internationally recognized best practices;

c) for developing organization-specific information security management guidelines.

ISO 27005

ISO/IEC 27005 provides guidelines for the establishment of a systematic approach to Information Security risk management which is necessary to identify organizational needs regarding information security requirements and to create an effective information security management system. Moreover, this international standard supports ISO/IEC 27001 concepts and is designed to assist an efficient implementation of information security based on a risk management approach.