Co-funded by the
Erasmus+ Programme
of the European Union

M08 Project Management and Management of risks

Study material

University of
Hradec Králové

TECHNICAL UNIVERSITY
OF KOŠICE

UNIVERSIDAD
DE GRANADA

Contents

List of Figures

Introduction

The module focuses on topics related to the project management process from the initialization phase, through planning, through implementation, and through monitoring to he finalization and evaluation phase. The module contains the basic components of the PRINCE2 methodology, which is one of recommended methodologies for the management of EU-supported projects. Special attention is paid to two components. The first is the Plan component with a focus on the project network analysis using the CPM method. The second component is Risk in the sense of risk management from the identification phase through risk assessment to the risk management phase. A project is a unique process consisting of a series of coordinated and managed activities with start and end dates, carried out to achieve a predetermined goal that meets specific requirements, including time, cost, and resource constraints. Projects are a way in which we change our economic, social and political situation in a structured way and develop our society.

Keywords

- Project management, IPMA, management of risk, PRINCE2 methodology, Gantt diagram.

Device Description and Specification

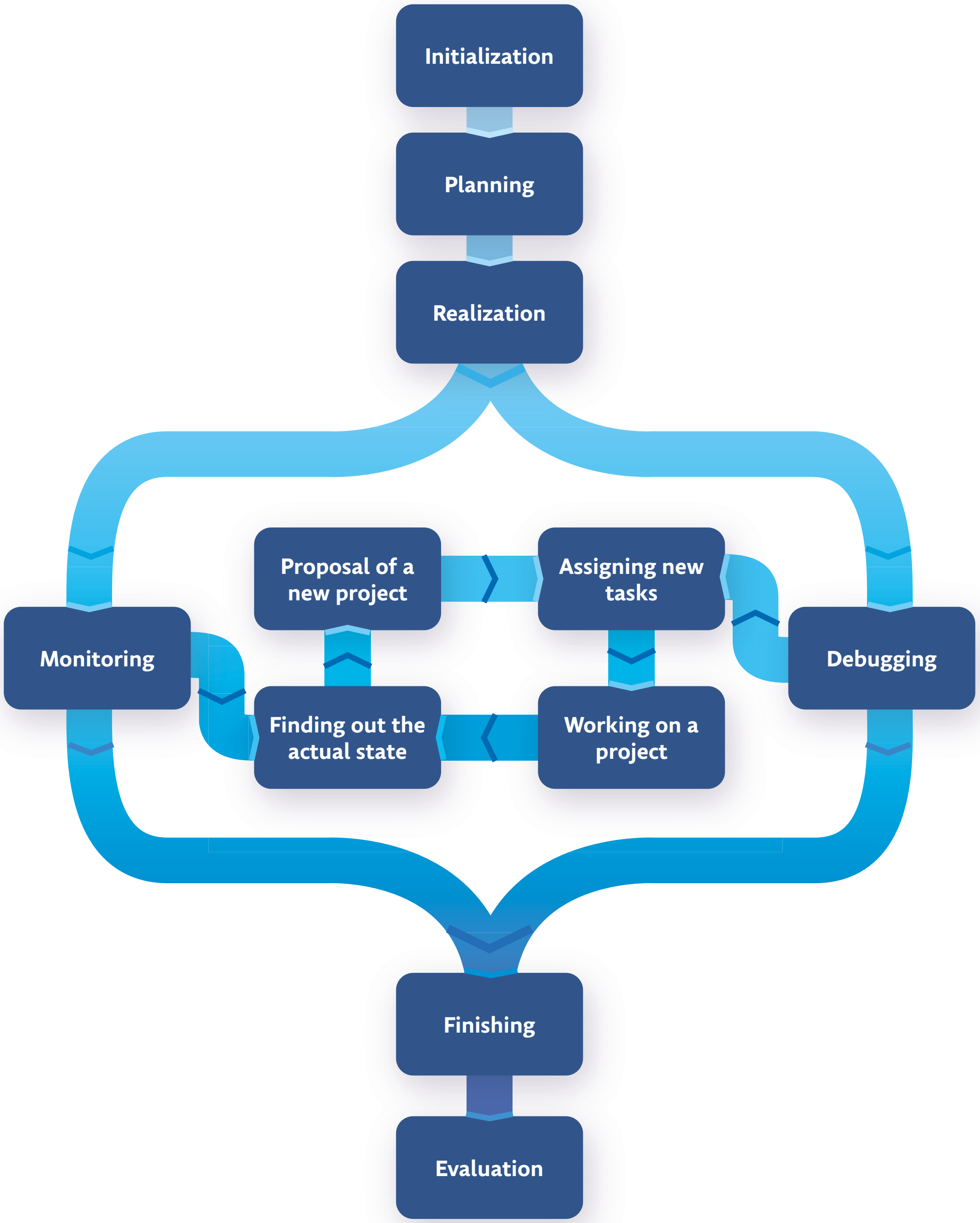

Figure 1: Stages of project implementation

If the creation of an organization as a start-up is not itself a project, but is a project within an existing organization, then it is usually significantly different from its normal operation. Key differences between a project and the day-to-day operations of an organization:

- Change – the project is a means of how to implement a change.
- Temporality – the project is only implemented for a set period of time until the desired change or outcome is achieved.

- Cross-functional – the project implementation team includes people with different specializations and from different parts of the organization, sometimes from different organizations. This brings different perspectives on how to deal with situations, different motivations for involvement (e.g., suppliers and customers), etc.
- Uniqueness – an organization may also implement projects that are similar in content, following a similar implementation scheme, but each project is unique (team composition, different customers, different location, ...).
- Uncertainty – the information stated above presents specific threats and opportunities for the project that are different from those arising from day-to-day operations. Projects are more risky.

Project initialization

The project initialization stage has two phases: the origin and development of the idea, the filtering of ideas. The first involves the idea of a possible project, discussing it with co-workers, gaining the support of superiors and partners, and then further developing and refining the idea. This phase is followed by a filtering phase, in which only the best ones are selected from the original large number of ideas. Before we even go into more detailed project planning, we need to answer a few basic questions with confidence:

1. Should the project be implemented at all?
2. Is the chosen implementation path correct?
3. Do we have the resources to implement the project?

Project planning

If the questions from the previous section are answered reliably and credibly, we can proceed with our own project planning. A number of techniques have been developed in project management for project planning. A very frequently used technique is to answer “W questions”, which has its origin in English methodologies. The project plan must answer the following questions:

- what?
  - the answer to this question describes the activities and (possibly) stages of the project,
- why?
  - answering this question characterizes the main objectives and impacts of the project,
- for whom?
  - the answer to this question characterizes the client, sponsors and the wider environment of project implementation,
- where?
  - the answer to this question indicates the location of the project,
- who?

    - the answer to this question characterizes the project implementer, resp. project team,
- when?
    - the answer to this question is the project schedule,
- with whom?
    - the answer to this question characterizes the project partners or other stakeholders,
- how?
    - the answer to this question characterizes the project implementation strategy, the process of this implementation, the method of its management, monitoring, and tuning, etc.,
- for how much?
    - the answer to this question brings the project budget.

The output of the planning phase should be a written document summarizing all relevant information, including a schedule. This document is binding for the subsequent implementation of the project.

The preparation of the project itself is usually subject to a set of rules. It is of course always necessary to comply with legal requirements and regulations, which are by their nature always fully binding, but project activities are usually further limited by a set of rules and guidelines specifying the actual implementation of the sub-project activities. In principle, a distinction can be made between projects in the private sector and projects financed by public budgets. In the first case, the implementation of the project and the form of the call are usually regulated by the internal regulations of the organization, while in the second case, which is more relevant in our context, the so-called tender documentation is crucial. It determines the exact and binding parameters for the implementation of the project, the way of its submission, etc.

Both types of projects should use a SWOT analysis in some form. This is a simple tool that allows for a quick orientation of the potential benefits and drawbacks of a project. The acronym is made up of English words:

- Strengths
- Weaknesses
- Opportunities
- Threats.

In principle, the SWOT analysis can be conceptualized quite simply as a list of items in the categories listed above. The purpose of the SWOT analysis is to enable a quick orientation in the issues of project solutions, or assessment of options. It is advisable to try to identify at least a few items in each category (not just one) to make the analysis sufficiently meaningful and useful.

The SWOT analysis also distinguishes between internal (S, W) and external (O, T) influences from the perspective of the organization's environment. Accordingly, we also speak about internal analysis and external analysis. In terms of the benefits/drawbacks for the project, a further distinction is made between positive (S, O) and negative (W, T) influences. Generally speaking, the positive impacts should prevail for the project to be meaningful. Positive impacts should be maximized, negative impacts minimized.

Project implementation and management

The implementation of the project consists in the gradual implementation of individual stages and the creation of products planned in these stages, in accordance with the set schedule and budget. Project management consists in assigning and controlling members of the project team, or partners, suppliers, etc., so that the set goals are achieved in the required quantity, quality, and deadline. The role of project managers is often described as monitoring the fulfillment of the so-called "three imperatives: WHAT, WHEN, FOR HOW MUCH". Optimally, these aspects are in balance, but if necessary, some of them can be accentuated, e.g., the project can be accelerated, but this can have a negative impact on other aspects (it can have a negative impact on quality). The PRINCE2 methodology extends the three-imperative to 6 aspects of project performance:

1. costs,
2. time,
3. quality,
4. scope,
5. risk,
6. benefits.

No project ever develops exactly according to its plan. In fact, the management of project implementation takes place in a cyclical way through a combination of tuning and monitoring. When monitoring the progress of the project, the factual situation and possible deviations from the original plan are continuously ascertained. Based on the comparison of monitoring results with the original plans, these plans are revised so that they still aim to achieve the project objectives.

There are different methodologies within project management that differ in their approach to roles and the triple bottom line. Within the PRINCE2 methodology, the following project roles are distinguished. The methodology lists several of them, only the essential ones will be mentioned here. It is worth noting that roles can overlap in the sense that one person has multiple roles within a project. However, the methodology explicitly states which roles are not compatible. The general principle is that if a role is a control role, it cannot be held by the subject of that control, i.e., the project manager cannot be a member of the project committee, etc.

Roles:

1. Project Committee: supervises the implementation of the project. According to the PRINCE2 methodology, it should include a senior user representative, a senior supplier representative, and a representative of the organization implementing the project. The project committee supervises the project design (e.g., whether it complies with the rules of the tender documents, the internal rules of the organization, etc.). The project committee is the body to which the project manager can escalate any problems that go beyond his/her powers.
2. Project Manager: runs the project on a day-to-day basis. S/he is responsible for the implementation of the project, the execution of the set plan, the achievement of the set objectives and outputs of the project. It may overlap with the role of team manager if it meets the qualification requirements in terms of specialization (typical especially for smaller projects).
3. Team Manager: handles the implementation of project work and generation of planned project outputs. The team manager leads a team of people who are qualified to implement the project plan. The team manager monitors the ongoing implementation and continuously reports the progress of the work to the project manager at pre-agreed time intervals.

Another widely used methodology is SCRUM. This is one of the agile methodologies and it focuses on rapid, incremental project implementation. Compared to the PRINCE2 methodology, SCRUM has a significantly simpler structure in terms of project roles:

1. Product owner: plays a key role in the SCRUM methodology. S/he adds additional tasks to the product backlog and above all checks whether the achieved outputs correspond to the required parameters/quality.
2. Team member: team members play a more important role in SCRUM than in PRINCE2 because they have a greater degree of autonomy. There is not such a rigid hierarchy, but they break down the tasks from the backlog and process them themselves.
3. SCRUM master: performs a supervisory function on the project, ensures that the project is implemented in accordance with the SCRUM principles and provides consultative support to the team and product owner.

The difference between the two models is that although they use the same inputs of the project triple-imperative – scope, cost, time, and intrinsic quality, the individual variables have different nature of fixed and variable variables.

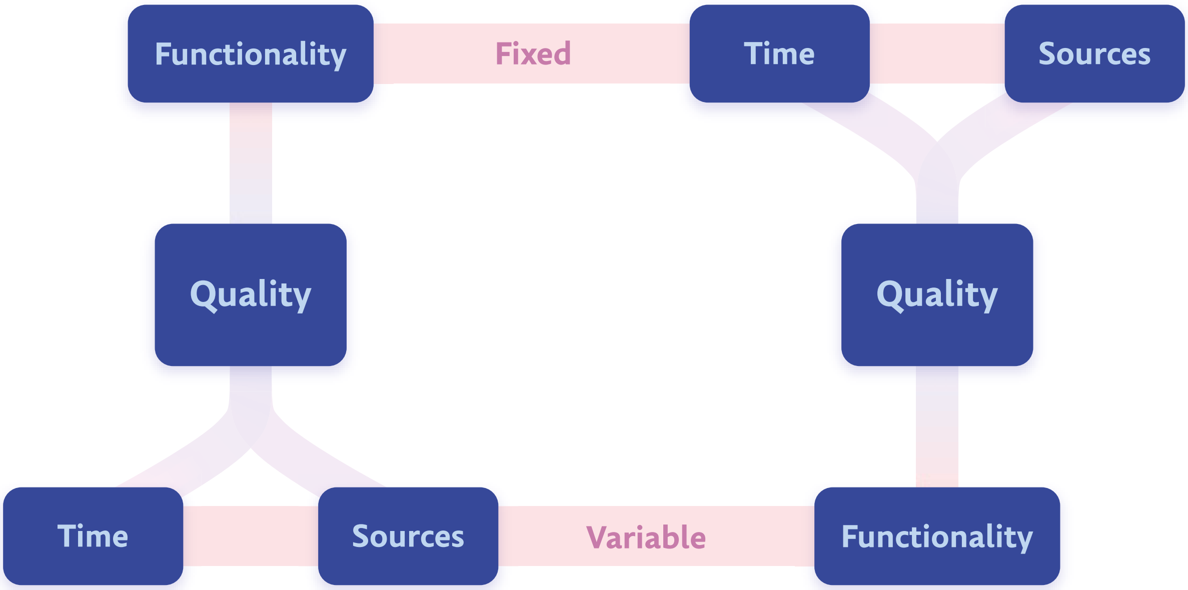

Figure 2: Agile approach

The biggest difference is that at the beginning of the traditional concept, the requirements are fixed. On the contrary, the agile approach has fixed time and resources and the requirements are expected to change. Another difference may be the relationship to risk. With short interactions, it is possible to track the diversification of risk during the project. This implies that the agile projects keep project risk at the same level without significant oscillations due to interactions.

Agile management is incremental, whereas in the classical concept it follows a predetermined and agreed project plan. The agile approach divides activities into shorter periods of time, called sprints, and work progress is reviewed continuously, often on a daily basis with the help of stand-up meetings. The classical approach then divides the project implementation into stages, with acceptance criteria for each stage, and the project is continuously implemented within a set timeframe.

The agile approach is more advantageous for project types where the outcome/goal state/output is more open or difficult to be specified in detail at the beginning of the solution. The classical approach, on the other hand, is easier in terms of time and financial management, as precise limits (financial and time) are given in advance.

Completion and evaluation of the project

Upon successful implementation of the project, there will always be a moment when the project is completed. This termination also has its rules. It is related both to the administration of the project itself and to the evaluation of its results. Completion of a project usually involves at least three basic activities:

- submission of the final project report,
- project billing,
- archiving of project documents.

Submission of the final report informs the project sponsor that the project has been completed and with what result. Its essential part is information about the progress of the project and about the achievement or non-achievement of project objectives.

Plan

The basic planning tool is the Gantt chart. It allows not only visualization of project processes for better understanding of key links, when the completion of one activity conditions the start of another, but more importantly, it allows project managers to track schedule performance. It is in the form of a table where all project activities are listed on the left side in sequence (ordered, if possible, in their logical sequence). As an example, a very simplified and optimistic conference organization project with four phases: planning, organization, implementation, and evaluation will be used. For each of them, we will define the individual tasks, their start, and completion dates.

Task	Duration	Start	Completion
Planning phase	**22 days**	**01.01.2021**	**31.01.2021**
Confirmation of conference location and date	1 day	01.01.2021	01.01.2021
Contacting the course leaders	7 days	04.01.2021	12.01.2021
Collecting commitments for event schedules	14 days		
Creating a graphic presentation of the conference	20 days	04.01.2021	29.01.2021
Negotiating booking details with accommodation partners	14 days	04.01.2021	21.01.2021
Organizational phase	**107 days**	**01.02.2021**	**29.06.2021**
Creating a web presentation	14 days	01.02.2021	18.02.2021
Public announcement of the conference	1 day	19.02.2021	19.02.2021
Promotional campaign	90 days	22.02.2021	25.06.2021
Planning and organization of a support event	7 days		
Organization of the final timetable	59 days	15.03.2021	03.06.2021
Publication of the full program	1 day	04.06.2021	04.06.2021
Departure of the location coordinator	2 days		
Implementation phase	**5 days**	**30.06.2021**	**06.07.2021**
Arranging the opening of the event	1 day	30.06.2021	30.06.2021
Conference	3 days	01.07.2021	04.07.2021
Completion and closure of the event	1 day	05.07.2021	05.07.2021
Evaluation phase	**20 days**	**05.07.2021**	**30.07.2021**
Sending a questionnaire about the conference to participants	1 day	05.07.2021	05.07.2021

Collection and evaluation of the questionnaires	11 days	06.07.2021	20.07.2021
Collection and processing of external data about the conference	14 days	05.07.2021	22.07.2021
Collecting and processing the team feedback	14 days	05.07.2021	22.07.2021
Evaluation of the success of the project	5 days	23.07.2021	29.07.2021

Table 1: An overview of project tasks – example – international scientific conference

The creation of the chart itself follows. The timeline in the chart is then placed in the appropriate box for the activity and the time period is marked whether or not the activity is taking place in that period. In addition, the links between the activities of the conditional type are displayed in the chart, i.e., whether the following activity is conditional on the outcome of previous activities and which ones. In our example, confirming the location and date of the conference is a precursor for contacting course leaders, developing a graphical presentation of the conference, and negotiating booking details with accommodation partners. Therefore, these tasks cannot start before the successful completion of the location and date confirmation. This follow-up is indicated by an arrow. When planning in, e.g., MS Project then the diagram takes the form of Figure 3.

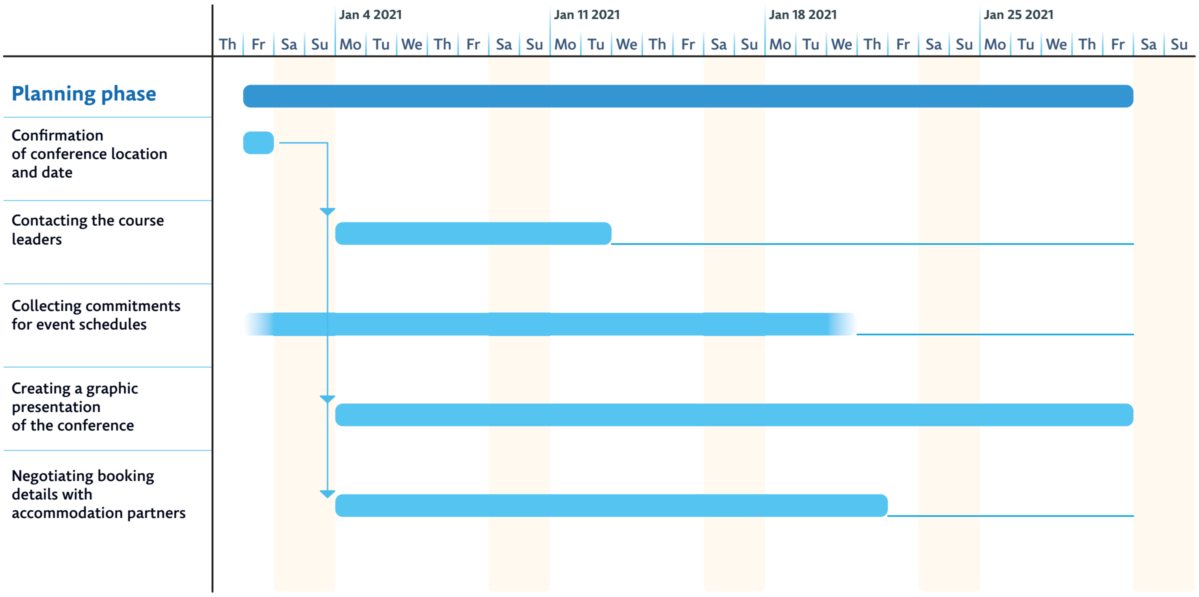

Figure 3: Chart of planning phase

The chart shows that not all tasks have a duration until the end of this phase. The phase is terminated by the task with the latest end date. The earlier end dates provide a time reserve, which can usually be indicated by a horizontal line. The successful completion of this phase is followed by the organization phase.

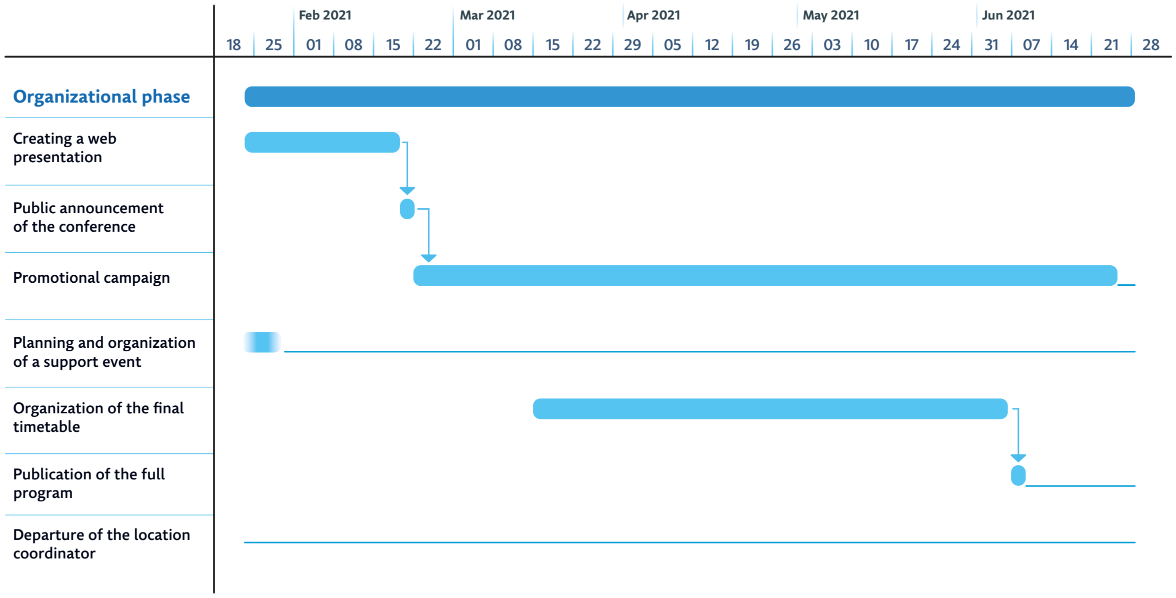

Figure 4: Chart of the organizational phase

The links to the previous and subsequent phases are marked with a black arrow and delimit the implementation dates of the phase. In this way, other tasks within the remaining phases are marked.

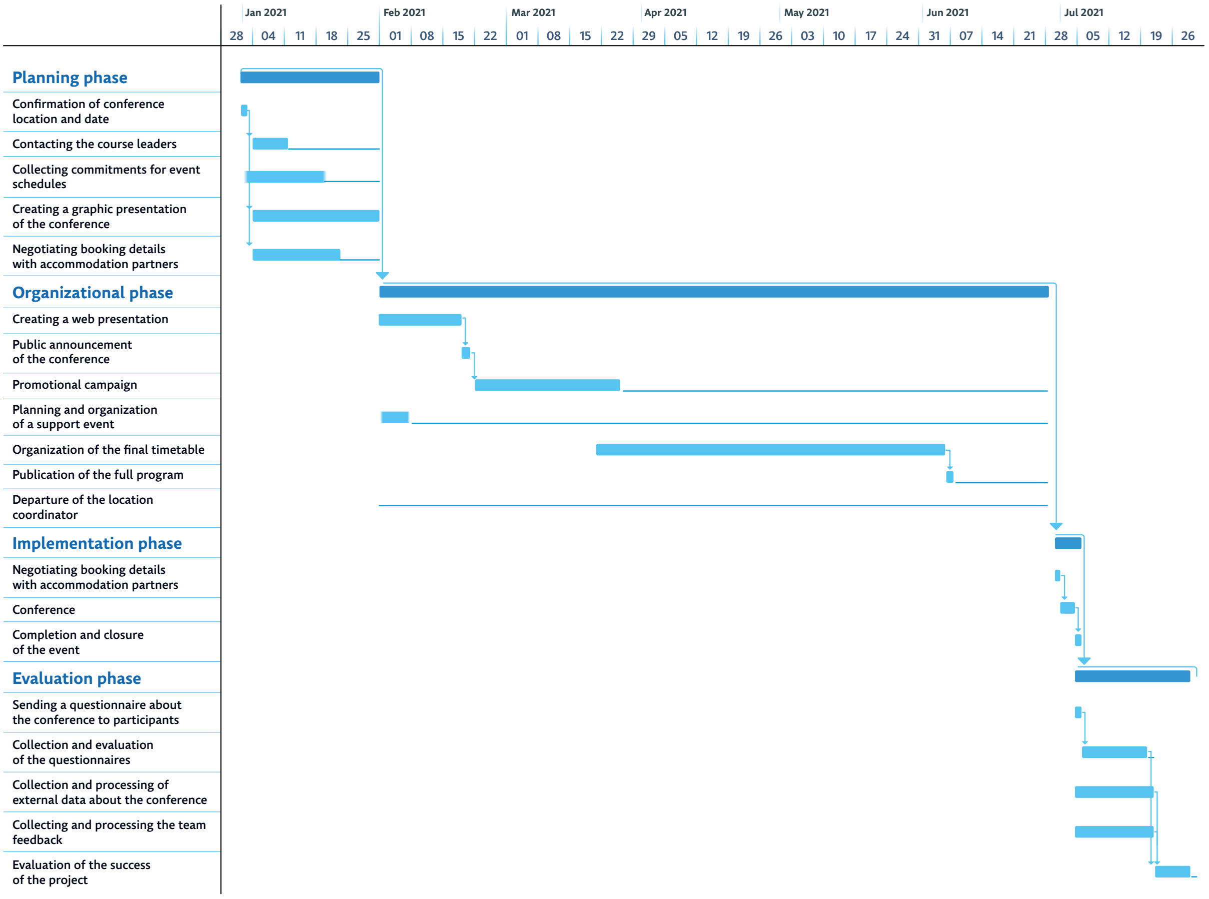

Figure 5: Chart of the conference project

Risk management

Risk management, risk mitigation or risk minimization and other similar terms are now increasingly used and inflected in various forms and contexts. Every organization or company operating in the field of security engineering faces risks in its activities that may lead to a reduction in the value of the organization, or even to its paralysis or complete destruction. Therefore, every manager tries to prevent the negative effects of these risks and, if they have already occurred, at least reduce their impact to the lowest possible level. We can say that risk management is always the focus of all important managers, because with its use it is possible to prevent large-scale losses and damages, which can have fatal consequences for the organization.

Terminological framework of risk management

The basic precondition for a successful solution of each issue is a precise and unambiguous definition of the terminological framework and possible existing deviations in the definition or understanding of certain terms. These deviations occur both as a result of a non-systemic solution to the problem, but above all as a result of its constant development. And it is this problem that also affects the area of risk management. Based on this, the following section defines the basic terms in accordance with standards ČSN ISO 31000 (2010) and TNI 01 0350 (2010) and selected professional publications (Smejkal and Rais, 2009).

The relationship between the basic terms defined in the area of risk management is shown in Figure 6. protected interests of the organization. These protected interests are threatened by external and internal threats, and these threats are triggered by threat sources, i.e. external factors or internal elements of the organization. The essence of the threat is to exploit the organization's vulnerabilities, overcome security measures and act on the asset where it will cause damage. The risk is then a quantification of the effect of threats on the assets and the residual risk represents a risk that still remains even after the introduction of security measures.

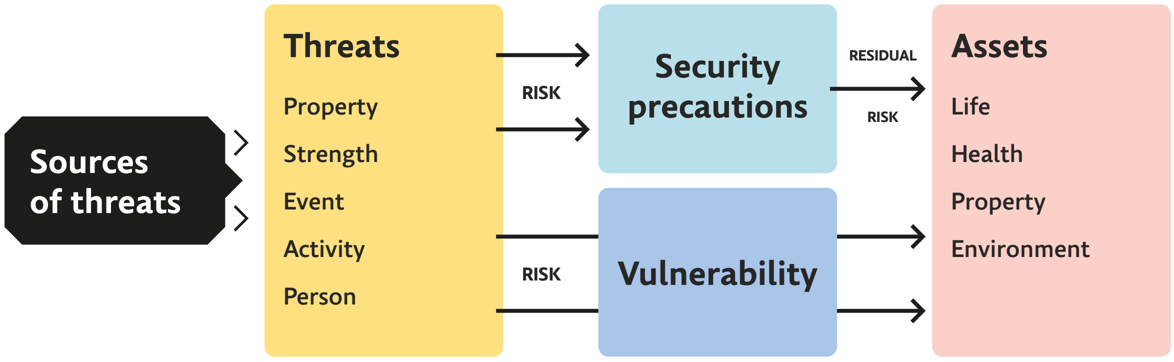

Figure 6: Relationship between basic terms in the field of risk management

Asset

By asset we mean everything that has some value for the organization, which can be reduced by the threat. Assets can be divided into two basic categories, namely tangible assets (e.g., funds, securities, real estate, etc.) and intangible assets (e.g., information, staff quality, copyright, etc.). However, the entity itself can also be an asset, as the threat can affect its entire existence. The asset has a certain vulnerability to exposure to the threat, which can be minimizedby implementing adequate security measures.

Threat Source

The source of a threat is any factor that can affect an organization's goals, processes, or projects. Thus, it is the external factors (e.g., external legislative environment, external political environment) or internal elements of the organization (e.g., processes, employees, real estate) that activate specific threats and whose development or activity (or inaction) are the causes of possible adverse effects to the assets of the organization.

Threat

By threat we mean a property, force, event, activity or person who acts either directly on the asset or on security measures in order to gain access to the asset. In order for a threat to work, it must first be activated, which is what the source of the threat is for. An alternative term, especially in the area of technological and health risks, is the concept of danger.

The basic characteristic of a threat is its level. The level of a threat is assessed according to three basic factors, which are danger (the threat's ability to cause damage), attitude (the probability that the threat will gain access to the asset) and motivation (the interest in initiating a threat to the asset).

Threats can be classified, in terms of the impact of threat sources on the organization, into two categories. The first category is external threats. These threats are uncontrollable, so in this category we can only mitigate the consequences of their actions. External threats can be further divided into six areas, namely political, economic, social, technological, legislative and environmental.This classification is performed according to the factors of PESTLE analysis (Grasseová et al., 2010), which serves for the analysis of the external environment. The second category is internal threats. These threats can be influenced, as in this category we can minimize or even eliminatethe causes of their effects. We can further divide the category of internal threats into three areas, namely process (project), personnel and material threats. The division of threats into categories and areas is shown in Figure 7.

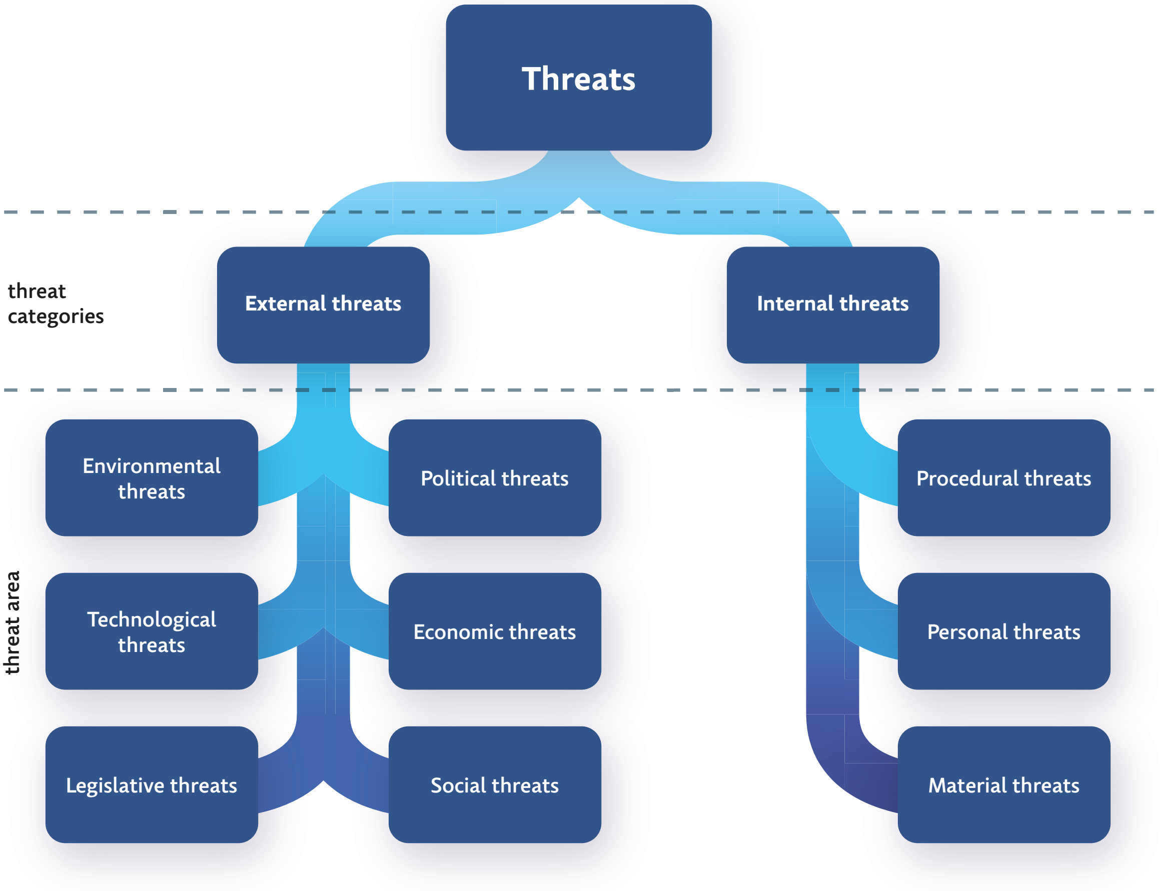

Figure 7: Breakdown of threats into categories and areas

The above-mentioned areas of external threats can be further divided into the following groups at a lower level of discrimination:

- In the area of political threats we can include, for example, the following groups of threats: intervention threats, threats associated with the change of state, threats associated with the change of government, threats associated with civic initiatives, but also war threats (military threats), regime threats (terrorism, extremism, separatism), proliferation threats (proliferation of weapons of mass destruction).
- In the area of economic threats, we can include, for example, the following groups of threats: budgetary threats, inflation threats, exchange rate threats, financial management threats (e.g., the collapse of banking institutions). For private companies, there are specific groups of business-related threats in this area of threats, such as investment or market threats.
- In social threats can include, e.g., the following groups of threats: demographic threat (overpopulation, mass migration), the threat level of education, cultural threats (ethnic and religious intolerance or discrimination), threats associated with unemployment, threats to health (diseases, injuries, etc.), criminal threats (arms trade, organized crime).

- In the area of technological threats we can include, for example, the following groups of threats: traffic threats, energy threats, communication threats, information threats (attack and misuse of critical information and information technology systems), industrial threats.
- In the area of legislative threats we can include, for example, the following groups of threats: threats associated with laws, decrees, standards or contracts, judicial threats.
- The following groups of threats can be included in the area of ecological threats: threats of natural disasters (natural disasters), threats of extraction of non-renewable resources, threats of ozone depletion, threats of increasing the greenhouse effect, threats of global warming, threats of climate change.

Similar to external threats, we can also divide internal threats at a lower level into the following areas:

- The area of process (project) threats can include, for example, the following groups of threats: threats related to process settings (e.g., non-existence or complexity of rules or internal normative acts for process implementation, non-existent or poorly defined process objectives, inappropriate process continuity, non-existent or poorly defined competence, inefficiency or inaccuracy of work procedures), threats related to process inputs (e.g., timeliness of inputs, quality of inputs), threats related to process resources (e.g., lack of resources, low or inappropriate quality of resources, poor allocation of resources), threats related to process outputs (e.g., timeliness of output deliveries, quality of outputs).
- In the area of personnel threats we can include, for example, the following groups of threats: qualification threats (e.g., ignorance, incompetence, poor training), ethical threats (e.g., bribery, conflict of interest, abuse of power, theft, fraud), threats associated with activities (e.g., inattention, negligence, incorrect operation, clumsiness).
- In the area of material threats we can include, for example, the following groups of threats: threats of a mechanical nature (e.g., noise, vibration), threats of a physical nature (e.g., heat, radiation), threats of a chemical nature, threats of a biological nature.

The above breakdown of assets and threats shows that organizations are affected by two categories of threats, external and internal. These threat categories can affect both tangible and intangible assets. At the same time, however, we must take into account that internal threats can also act outside the organization, on the assets of other organizations. The scheme of the effect of threats on assets is shown in Figure 8.

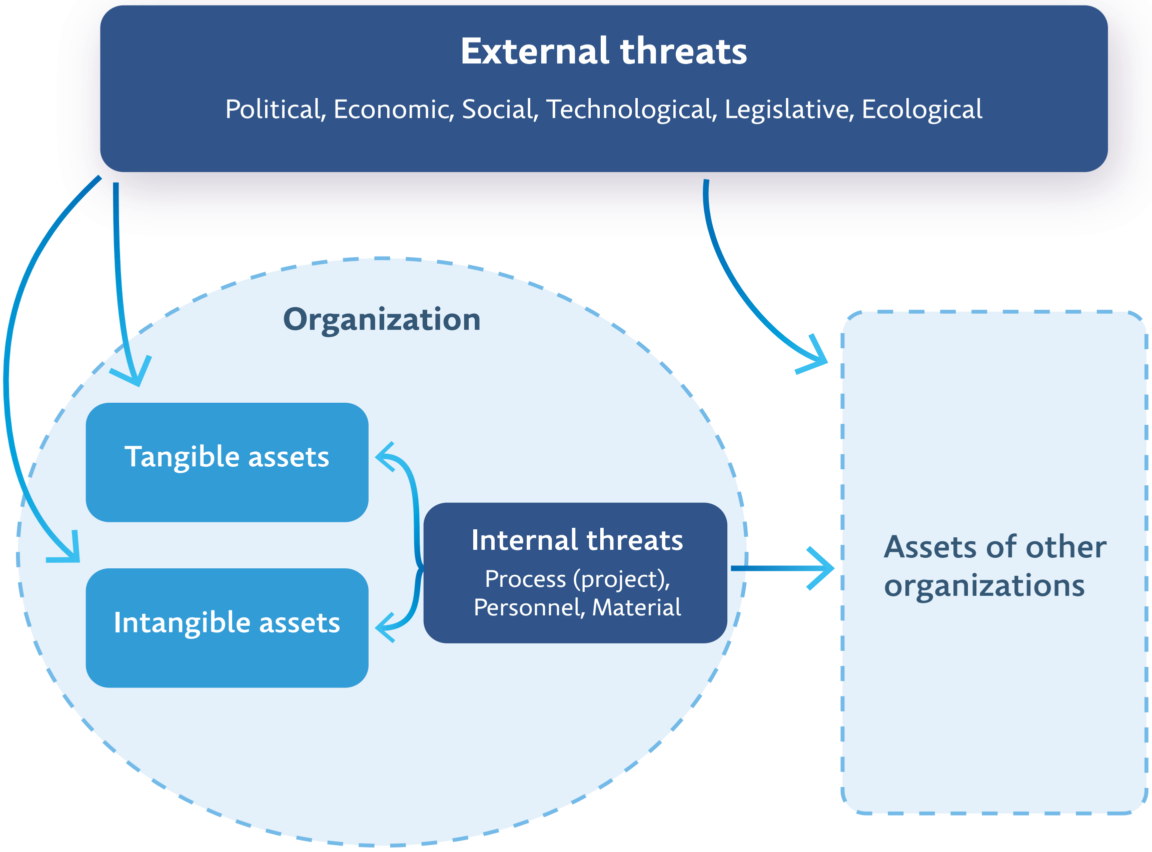
External threats
Political, Economic, Social, Technological, Legislative, Ecological
Organization
Tangible assets
Intangible assets
Internal threats
Process (project), Personnel, Material
Assets of other organizations

Figure 8: Scheme of the effect of threats on assets

In connection with the impact of threats on assets, it is important to note that most elements of the organization (e.g., processes, employees, real estate) can act in two roles. On one hand, they may represent assets that are affected by external and internal threats. At the same time, however, they may themselves have a negative effect on the organization's other assets, and at this point they are already acting as internal sources of threats.

Risk

The risk arises from the interaction of the threat and the asset and is expressed by the combination (or product) of the probability of occurrence of the extraordinary event and its impact on the given asset. We can therefore understand risk as quantifying the effect of a threat on an asset. We can also state that the risk is the possibility that in the provision of the organization's activities with a certain probability will occur a certain extraordinary event with subsequent adverse effects on the fulfillment of the approved intentions and goals of this organization.

Example: The basic relationship between the terms threat, source of threat and risk is demonstrated on the example of a terrorist attack, which is still a very current threat in the current security environment. A specific threat may be, for example, the hijacking or destruction of a fully occupied XY aircraft (in this case, the asset is both the aircraft itself and the crew, passengers *and cargo carried). The source of the threat in this case is the supporters of the terrorist group or organization. The risk is the product of the probability that the aircraft will be hijacked or destroyed and the severity of the impact of this emergency.*

Risks can be classified according to the material content into various types, which are named according to the relevant type of threat that affects the assessed assets of the organization. These are, for example, political risks, economic risks, social risks, etc. Some professional publications (Smejkal and Rais, 2009; Tichý, 2006) also state the classification of risks according to other classification aspects such as:

- in terms of predictability, i.e., risks predictable and unpredictable

Example: A typical example of a predictable type in organizations may be the risks arising from the handling of classified or confidential information. Natural events are an example of relatively unpredictable risk, and terrorist attacks, for example, are almost unpredictable.

- in terms of manageability, i.e., risks that can be influenced and cannot be influenced

Example: Natural events are a typical example of uncontrollable risks, as in these cases the organization can only mitigate the effects of adverse events (e.g., in the case of flood protection by building flood defenses or by relocating the organization's headquarters outside the floodplain).On the other hand, an example of an manageable risk is, for example, the risk of concluding a unilaterally unfavorable contract, which we can prevent, for example, by renting the services of a professional consulting or law firm in a given area.

- in terms of origin, i.e., primary and secondary risks, the primary risks being the original, while the secondary risks are triggered by the implementation of measures to mitigate the primary risks

Example: In the case of leasing the services of a professional consulting firm, the primary risk of concluding a unilaterally unfavorable contract is minimized. On the other hand, there may be a secondary risk associated with the misuse of the information that will be provided to the consulting firm in the proceedings.

- in terms of objectivity of evaluation, i.e., subjective and objective risks
- in terms of the dynamics of the development of the adverse event, i.e., risks slow and fast
- in terms of the probability of the occurrence of an adverse event, i.e., probable and unlikely risks
- in terms of the intensity of the impact of the adverse event, i.e., the risks with a mild, higher and fatal impact.

Vulnerability

A vulnerability is a deficiency, weakness, or condition in an analyzed asset that a threat can exploit to exert its adverse effects. This quantity is a property of the asset and expresses how sensitive the asset is to the effects of the threat. Vulnerability arises where there is an interaction between a threat and an asset, and the basic characteristic of vulnerability is its level. This is determined according to two basic factors, namely sensitivity (susceptibility of the asset to be damaged by the threat) and criticality (significance of the asset to the analyzed organization).

Example: In the event of a threat of hijacking or destruction of a fully occupied aircraft, the possibility of bringing small luggage with personal belongings on board the aircraft or inconsistent security measures at individual European airports can be considered vulnerable.

Security Measures

A precautionary measure is a process or means designed to minimize the effects of a risk that can be achieved by:

- reducing the vulnerability of the asset,
- eliminating sources of threats,
- reducing the likelihood of an emergency,
- reducing the severity of the impact of the emergency.

Security measures protect assets or detects the impact of threats and mitigates or completely prevents their impact on assets. In terms of risk analysis, security measures are characterized by effectiveness and cost. This means that when designing these measures, the costs incurred to reduce the risk should be commensurate with the value of the protected assets.

Example: In the example of the threat of hijacking or destruction of an aircraft, we will once again consider security measures such as the existence of at least existing measures at airport terminals or increasing security during the flight itself by armed police officers who are placed on board the aircraft on selected riskiest flights among ordinary passengers.

Residual Risk

Residual risk is a risk that has not been addressed or still remains after safety measures have been implemented. The residual risk should be so low as not to exceed the risk reference level and should be acceptable to the organization so that no additional security measures need to be put in place to reduce it. The reference level of risk represents the chosen and widely accepted limit of the level of risk, which is either enshrined in legislation, standards and industry norms, or has been set by the organization. This level is used to assess whether the residual risk is acceptable or not tolerable for all stakeholders.

Consequences

The significance of the impact of a threat may be derived from the absolute value of the losses, which includes the cost of restoring the asset or the cost of removing the damage caused to the organization by the threat.

Extraordinary Event

By extraordinary event we mean an unfavorable (undesirable) deviation from the expected (desired) result or state, resp. a serious, time-difficult and spatially limited event caused by anthropogenic activity, natural influences or processes that endangers life, health, property or the environment. In the field of technological risks, the term accident is used for this term.

Risk Management

Risk management is the process by which an organization or entity seeks to prevent existing or anticipated threats and proposes solutions to minimize the severity of the impact and/or the likelihood of incidents through appropriate security measures.

Example: The practical interpretation of the whole terminological framework mentioned above is clearly demonstrated on the example of occupational safety and health (OSH) of employees of the organization who work in the office. One of the threats to these workers (i.e., assets) isdue to their safety possible electric shock (i.e., threat) when handling electrical appliances. The source of this threat in this case is the electricity itself and the extraordinary event of workers being hit by this current. The level of risk of electric shock to workers is then determined by a combination of the probability with which they may be affected (e.g., in case of unprofessional handling of electrical appliances the probability of electric shock is higher than in compliance with established rules) and severity of impact (e.g., in case of electric shock 380 V there would be more extensive injuries to the affected person than if affected by an electric current of 230 V). In this case, we can consider, for example, performed health and safety training or inspection of electrical equipment (this is a reduction in the probability of electric shock) or timely provision of first aid (this is a reduction in the severity of the impact already in the event of electric shock). On the contrary, we can consider as vulnerability, for example, poor grounding of electrical appliances or insufficient training of employees of the organization in the field of first aid.

Risk management process

The risk management process must be an integral part of the organization's management, it must be embedded in the culture and practice of the organization and it must be adapted to its processes.The risk management process consists of five basic sub-processes (see Figure 9), which are communication and consultation, context definition, risk assessment (includes risk identification, analysis and assessment), risk management and process monitoring and review. These activities are described in the following text.

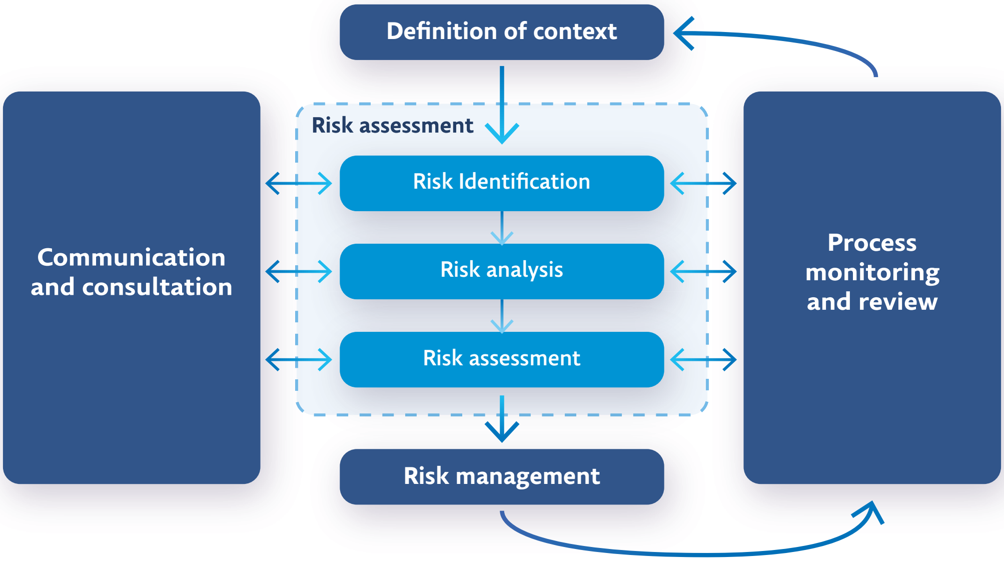

Figure 9: Risk management process (adjusted according to ČSN ISO 31000: 2010)

Communication and consultation

Entry into the subprocess: Implemented risk management framework.

Subprocess activities:

1. Elaboration of communication and consultation plan
2. Implementation of effective communication and consultation with internal stakeholders
3. Implementation of effective communication and consultation with external stakeholders

Subprocess output: Processed communication and consultation plan.

Communication and consultation with internal and external stakeholders must be an integral partof every subprocess in the risk management process. Based on this, we should develop a communication and consultation plan, both with internal and external stakeholders, at an early stage. This plan should address not only the risks themselves, but also their effects (if known) and the measures taken to manage them. The communication and consultation plan is a tool for exchanging information between stakeholders and for conveying messages that are true, accurate, understandable and evidence-based.

As part of the risk management process, we should implement effective internal and external communication and consultation to ensure that those responsible for implementing the risk management process and stakeholders understand the nature and rationale for why individual actions are required and make appropriate decisions accordingly. The teamwork approach is especially useful when: defining context in an adequate way; ensuring that the interests of stakeholders are understood and considered; gathering different areas of expertise for risk analysis; ensuring that risks are fully identified; ensuring that different views are adequately considered in the risk assessment; improving appropriate change management during the risk management process; securing approval and support for the risk management plan; or developing an appropriate plan for internal and external communication and consultation.

Communication and consultation with stakeholders is very important as stakeholders make risk judgments based on how they perceive those risks. Risk perceptions may change due to differences in the values, needs, assumptions, concepts and interests of stakeholders. As stakeholder requirements, expectations and influences can have a significant impact on the decisions made, it is important that stakeholder judgments are identified, recorded and taken into account in the decision-making process.

Defining the context

Entry into the subprocess: Elaborated plan of communication and consultation.

Subprocess activities:

1. Definition of external contexts
2. Definition of internal connections

3. Defining the limits of risk management
4. Establishing criteria for risk assessment

Subprocess output: Defined internal and external factors, defined risk management limits and set criteria for risk assessment.

By defining the context of the organization, we define the internal and external factors that we should take into account in risk management, and set the scope and risk criteria for the remaining process. These contexts should include both internal and external factors relevant to the organization. Although many of these factors are similar to those considered when designing the risk management framework, we need to consider these factors in more detail and depending on the scope of the risk management process when defining the context of the risk management process.

First, we **define the external context**. By external context we mean the external environment in which the organization strives to achieve its goals. Understanding the external context is important to ensure that external stakeholders, their objectives and interests are considered when setting risk criteria. This is based on the broader context of the organization, but in line with the specific details of legal requirements, stakeholder perceptions and other aspects of risk characteristic of the scope of the risk management process. External contexts include, as in the case of the risk management framework, the expectations of external stakeholders and trends affecting the organisation's objectives arising from the political, economic, social, technological, legislative, environmental and competitive environments.

Subsequently, we **define the internal context**. By internal context we mean the internal environment in which the organization strives to achieve its goals. The risk management process should be in line with the culture, processes and structure of the organization. Internal contexts are anything within an organization that can affect the way the organization manages risk. It is necessary to define these contexts precisely, because risk management is implemented in the context of the organization's goals. At the same time, the objectives and criteria of the specific project or process/activity need to be considered in relation to the objectives of the organization as a whole. The main risk for some organizations is the failure to achieve their strategic, project or specific goals, and it is the risks that affect the fulfillment of the contractual obligation, reliability, trust and values of the organization.

In the next step, we will **define the boundaries of risk management**. The basic premise of defining the boundaries of risk management in an organization is to define the goals, strategies, scope and factors of those activities, processes or parts of the organization where the risk management process will be applied.

Lastly, we will **set criteria for risk assessment** or risk criteria. Within the organization, we should define criteria that will be used to assess the significance of risks. These criteria reflect the values, goals and resources of the organization. Some criteria may be derived from legal requirements or other requirements to which the organization agrees. The risk assessment criteria must be consistent with the organisation's risk management policy, must be developed at the beginning of each risk management process and must be constantly reviewed. When defining risk criteria, it is necessary to consider some important factors, such as:

- the nature and type of impacts that may occur, including how they are measured,
- probability determination method,
- time frame of probability and/or impacts,
- the method of determining the level of risk,
- the level at which the risk becomes acceptable and tolerable,
- the level of risk required to manage it,
- whether a combination of multiple risks should be taken into account.

The context of the risk management process will vary depending on the needs of the organization, which may include defining responsibilities for the risk management process, defining the framework and scope of risk management activities to be performed (including their specific involvement in or exclusion), defining activities, processes, functions, projects, products, services or assets (in terms of time and location), as well as the purpose and objectives of the organization, defining the relationship between a particular project or activity and other projects or activities of the organization, defining methodologies for risk assessment, defining the method how risk management performance is assessed and the decisions that need to be made are identified and specified. The attention paid to these and other important factors helps to ensure that the approach to risk management adopted is appropriate to the situation and to the risks affecting the achievement of the organization's objectives.

Risk assessment

Entry into the subprocess: Defined internal and external factors, defined limits of risk management and set criteria for risk assessment.

Activities and actions of the subprocess:

1. Risk identification
    1. Asset identification, asset valuation and asset grouping
    2. Identification of threats and sources of threats
2. Risk analysis
    1. Threat and vulnerability analysis
    2. Determining the severity of the impact of an adverse event
    3. Determining the probability of an adverse event
    4. Determining (estimating) the level of risk
3. Risk assessment
    1. Comparison of specified risk levels with specified criteria
    2. Determination of risk acceptability

Subprocess output: List of prioritized acceptable and unacceptable risks that will be further managed.

The next sub-process after defining the context is risk assessment, which includes three core activities, namely risk identification, analysis and assessment. The initial activity of the risk assessment subprocess is **risk identification**. As part of this activity, we perform two tasks, namely identification, determination of value and grouping of assets (action 1.1) and identification of specific threats and possible causes of their operation, i.e., sources of threats (action 1.2). The aim of this step is to create a comprehensive list of risks based on such events that could prevent, reduce or slow down the achievement of goals. It is also important to identify the risks associated with not taking advantage of the opportunity. However, a necessary step in identifying risks is to consider all possible causes. Comprehensive identification is crucial because risks that are not identified at this stage will not be included in the following analysis. Therefore, up-to-date information, which should include appropriate and detailed data, is important in identifying risks. The identification thus includes all risks, regardless of whether their source is already under the control of the organization or not yet.

Asset identification consists in creating an inventory of all assets within the risk management boundary, which we defined in the previous subprocess. When deciding on the inclusion of a given asset in the inventory, the name of the asset and its location shall be stated (e.g., a Tatra 815 car, located in the underground garages of block C8). The following determination of the value of an asset is based on the amount of damage caused by the destruction or loss of the asset. Usually, the value of an asset is determined on the basis of its cost characteristics (acquisition prices, reproduction acquisition prices), but they can also be revenue characteristics (if the asset brings well-identifiable profits or other significant benefits for the entity). Revenue characteristics also include the characteristics of the asset used to make profits indirectly – for example, market position, trademark, but also the qualifications and know-how of employees. It is very important to distinguish whether it is a unique asset or an easily replaceable asset. The value reflects the entity's dependence on the existence, but also on the proper functioning of the assessed asset, i.e., what damages will occur due to reduced functionality or loss of the asset before it is restored. The value of an asset for risk analysis may also be determined as a weighted average of the values used in all aspects. Since there are usually a large number of assets, their number is reduced by grouping the assets according to different aspects in order to create groups of assets with similar characteristics. Assets of similar quality, price, purpose, etc. can be grouped. The group of assets thus created then further acts as one asset. It is then necessary to ensure that the security measures proposed in the risk management stage for a group of assets are applied to all assets that are grouped into that group. (Smejkal and Rais, 2009)

The identification of threats and their sources is performed by selecting those threats and their sources that may threaten at least one of the entity's assets. To identify threats and their sources, it is possible to use a list of threats, compiled according to the available literature, own experience, surveys or previously performed analyzes. Threats can also be derived from the entity, its status (business entity, government organization, non-profit organization, etc.), market position, economic results, intentions of the entrepreneur. (Smejkal and Rais, 2009)

The second activity after risk identification is risk **analysis**, which is based on improving the understanding of risks. It provides inputs for risk assessment and for deciding whether identified risks need to be managed and what are the most appropriate risk management strategies and methods. Risk analysis takes into account the causes and sources of threats, their positive and negative impacts (consequences) and the probability that these impacts may occur. Factors that affect the severity of the impact and the likelihood of an event should also be identified. The result of risk analysis is the determination or estimation of individual risk levels.

The first task performed within the risk analysis activity is the analysis of threats and vulnerabilities (action 2.1). Each threat is assessed against each asset or group of assets. For those assets to which a threat may be applied, the level of threat to that asset and the level of vulnerability of the asset to that threat shall be determined. Factors such as danger, motivation and attitude are taken into account when determining the threat level. Factors such as sensitivity and criticality are used to determine the level of vulnerability. The implemented security measures are taken into account when analyzing threats and vulnerabilities. These measures can reduce both the level of threat and the level of vulnerability. The resulting status is a list of "threat-asset" pairs (only those pairs where a threat can be applied to an asset) with a specified level of threat and vulnerability (Smejkal and Rais, 2009).

In the second and third actions, we then analyze the risk by determining the impacts (action 2.2) and their probabilities (action 2.3), or other risk attributes, bearing in mind that the event may have multiple impacts and may affect multiple objectives. The risk analysis should also take into account existing risk control and its effectiveness. The way impacts and probabilities are expressed and the way they are combined to determine the level of risk varies according to the type of risk, the information available and the purpose for which the result of the risk assessment is to be used. This approach should be in line with risk criteria, which is also important to consider the interdependence of different risks and their sources. Reliance on the determination of risks and their sensitivity based on preconditions and assumptions should be duly considered in the analysis and communicated to management entities and, if necessary, other stakeholders. All factors of risk analysis, such as differences of opinion among experts or limited risk modeling, should be noted and duly emphasized.

We can perform a risk analysis with varying degrees of detail, depending on the specific risk, the purpose of the analysis, and the sources of information available. We can perform the analysis in a qualitative, semi-quantitative or quantitative way or a combination of them, depending on the requirements and availability of information. In practice, qualitative analysis is often used first to obtain general data on the level of risk and to identify the main risks. If possible, a more objective semi-quantitative or quantitative risk analysis should be performed in the next step. The type of analysis chosen must also comply with the risk assessment criteria set out in the context definition.

Qualitative analysis uses verbal evaluation to describe the severity of potential impacts and the probability with which those impacts will occur (see Table 2). Qualitative evaluation scales can be adapted or adjusted to suit the circumstances, e.g., different descriptions can be used for different risks. Qualitative analysis can be used as an initial activity to identify risks that require more detailed analysis, or where this type of analysis is suitable for decision making, or where numerical data or sources are not adequate for quantitative analysis.

In the **semi-quantitative analysis**, the corresponding values are assigned to the qualitative scale, i.e., point scale of the scale (see Table 2). The aim is to create a wider rating scale than is usually used in qualitative analysis, but not to design realistic values for risk calculation as in the case of quantitative analysis. Increased attention should be paid to the implementation of the semi-quantitative analysis, as the selected numbers may not correspond to reality, which may lead to conflicting, deviating or disproportionate results. Semi-quantitative analysis may not correctly distinguish risks, especially when the impact or probability reaches extreme values.

Quantitative analysis uses numerical values that are much more accurate than the descriptive scales used in qualitative and semi-quantitative analysis (see Table 2). Data from various sources are used to express the severity of the impact and the probability of occurrence. The value of the asset (if it is assumed that it will be completely destroyed) or the costs required to repair the damage (i.e., to reconstruct or restore the asset) are most often used to quantify the severity of the impact.In the case of probability, we can speak of a quantitative expression if the actual frequency or probability of occurrence of a certain event is known. The quality of the analysis then depends on the accuracy and completeness of the numerical values and the validity of the models used.

However, impacts can also be determined by modeling the results of an event or set of events or by extrapolating experimental research or available data, and can be expressed in terms of tangible and intangible impacts. In some cases, the specification of impacts for different times, places, groups or situations is required to be implemented by more than one numerical value or descriptive element.

	Qualitative analysis	**Semi-quantitative analysis**	**Quantitative analysis**
Probability of occurrence	high	4	83 %
Impact severity	medium	3,5	120,000 $

Table 2: Example of expressing values in individual types of risk analysis

Legend:

For simplicity, the severity of the impact is expressed only by the value of the analyzed asset.

Qualitative analysis – expression through verbal evaluation.

Semi-quantitative analysis – expression through a point scale, e.g., from 1 to 5

Quantitative analysis – expression through actual values (i.e. the amount of probability in percent and the severity of the impact in money)

The last task of the risk analysis activity is to determine or estimate the level of risk (action 2.4). The way in which the impacts (consequences) and probability are expressed and combined in order to determine the level of risk varies according to the type of risk and the purpose for which the outputs of the risk assessment are used. However, usually the risk level (R) is calculated as the product of the severity of the impact (D) and the probability of occurrence (P) divided by the safety measures (B) - see relation (1).

$$R = \frac{D \times P}{B} \tag{1}$$

The final activity of the risk assessment subprocess is **risk assessment**. The purpose of this activity is to assist in deciding (based on the results of risk analysis) which risks must be managed as a matter of priority. Risk assessment involves two actions, namely the comparison of risk levels determined during the analysis with the risk assessment criteria established in the context definition (action 3.1) and the subsequent determination of risk acceptability and their prioritization (action 3.2). If the level of risk does not meet the set criteria, the risk must be managed. When deciding to initiate a risk management subprocess, we should consider the broader context of the risk and take into account the allowable deviation for risks arising in the external environment of the organization. We should then make the decision in accordance with legal or other accepted requirements. In some circumstances, a risk assessment may lead to a decision to perform further analysis or to decide not to address risk management in any way other than maintaining existing risk regulation.This decision is generally influenced by the organization’s interest or attitude to the risks and risk criteria that have been established.

At the end of the description of the risk assessment subprocess, an overview and applicability of risk assessment tools are presented, i.e. for their identification, analysis and evaluation (see Table 3).

Tools and techniques	**Risk assessment subprocess**				
	Risk identification	**Risk analysis**			**Risk assessment**
		Severity of impact	**Probability**	**Level of risk**	
Brainstroming	1	3	3	3	3
Structured or semi-structured interviews	1	3	3	3	3
Delphi method	1	3	3	3	3
Checklists	1	3	3	3	3
Preliminary hazard analysis	1	3	3	3	3
Hazard and Operational Studies (HAZOP)	1	1	2	2	2
Hazard Analysis and Critical Control Points (HACCP)	1	1	3	3	1
Environmental risk assessment	1	1	1	1	1

Structure “What happens when?” (SWIFT)	1	1	1	1	1
Scenario analysis	1	1	2	2	2
Business impact analysis	2	1	2	2	2
Root cause analysis	3	1	1	1	1
Analysis of ways and consequences of failures	1	1	1	1	1
Fault state tree analysis	2	3	1	2	2
Event tree analysis	2	1	2	2	3
Cause-effect analysis	2	1	1	2	2
Analysis of causes and consequences	1	1	3	3	3
Analysis of protection layers (LOPA)	2	1	2	2	3
Decision tree analysis	3	1	1	2	2
Analysis of trouble-free human activity	1	1	1	1	2
Butterfly type analysis	3	2	1	1	2
Fault-tolerant maintenance	1	1	1	1	1
Analysis of parasitic phenomena	2	3	3	3	3
Markov analysis	2	1	3	3	3
Monte Carlo simulation	3	3	3	3	1
Bayesian statistics and Bayesian networks	3	1	3	3	1
FN curves	2	1	1	2	1
Risk indices	2	1	1	2	1
Matrix of consequences and probabilities	1	1	1	1	2
Cost-benefit analysis	2	1	2	2	2
Multicriteria Decision Analysis (MCDA)	2	1	2	1	2

Table 3: Applicability of risk assessment tools (modified according to ČSN EN 31010: 2011)

Legend:

1 – Very good to use

2 – Useful

3 – Not usable

Risk management

Entry into the subprocess: List of prioritized acceptable and unacceptable risks that will be further managed.

Subprocess activities:

1. Choosing the most appropriate risk management option
2. Implementation of risk management plans
3. Ensuring the feasibility of selected security measures
4. Determination of residual risk acceptability

Subprocess output: List of residual risks with an acceptable level.

Risk management involves selecting one or more risk minimization options and implementing them. It is a cyclical subprocess of the risk management process, which involves assessing risk management and then deciding whether or not the residual level of risk is acceptable. If the risk is not acceptable, we need to re-manage the risk and reassess its effectiveness. This subprocess lasts until the residual risk reaches a level corresponding to the set risk assessment criteria. The individual risk management options are not necessarily mutually exclusive or may not be appropriate in all circumstances. The individual risk management options are shown graphically in Figure 10.

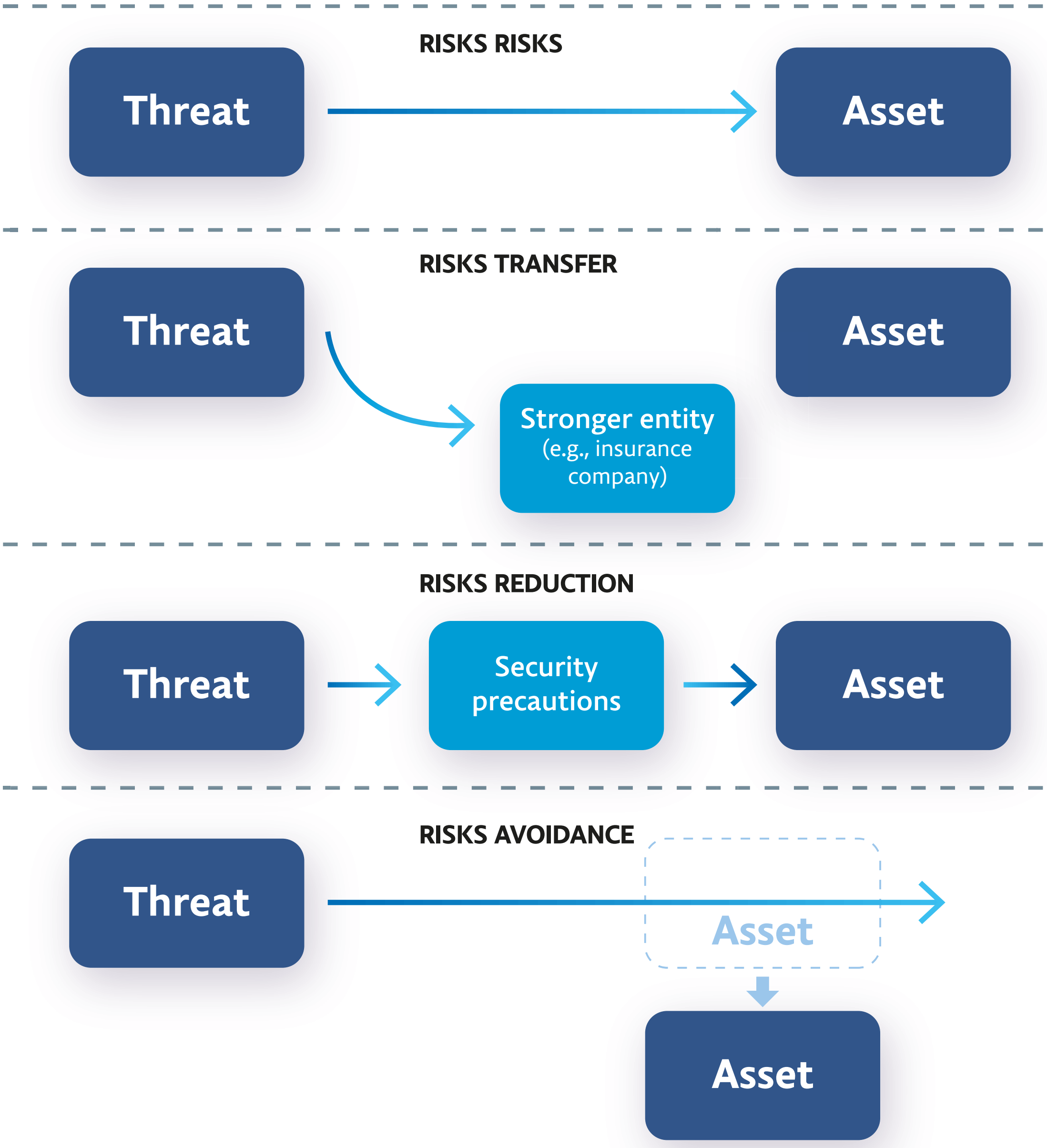

Figure 10: Risk management options

Risk Retention is a legitimate and probably the most common method of risk management. It is that the organization faces an almost unlimited number of risks, but in most cases does nothing against them. Risk retention can be conscious or unconscious. Conscious risk retention occurs when a risk is recognized and one of the other risk management options is not applied (e.g., in the form of its transfer or reduction). If the risk is not recognized, he is unknowingly detained. In these cases, the organization does not address the consequences of possible losses, as it is not even aware of their occurrence. Risk retention can also be voluntary or involuntary. Voluntary risk retention is characterized by recognizing the existence of risk and tacit consent to accept the loss contained in it. The decision on voluntary risk retention is made because there are no better options. Involuntary risk retention exists when risks are unknowingly retained, or when the risk cannot be transferred or reduced, or if it cannot be avoided. (Smejkal and Rais, 2009)

Risk Reduction can basically be implemented in two approaches. The first approach is to reduce the likelihood of an adverse event. This is an offensive approach based on the implementation of preventive measures. The second approach is to reduce the severity of the impact (consequences) of an adverse event that has already occurred and to speed up the reconstruction of the affected asset. In this case, it is a defensive approach based on ex-post measures. In both approaches, the risks can be minimized either on the source side of the threat or on the asset side. In general, the best combination of the above risk reduction options is to reduce the likelihood of an adverse event occurring on the source side. Elimination of the source of the threat (e.g., complete eradication of terrorist groups and organizations) can be considered the optimal, but at the same time also the most demanding and almost unfeasible option.

Risk Transfer is one of the options that is characterized by a defensive approach to risk. It is a transfer of risk to another entity that is economically stronger. Thus, risk transfer does not eliminate the causes of an adverse event (e.g., the removal of competition from the market by economic or political force), but focuses only on mitigating its potential effects. Taking various types of insurance can be considered the most typical example of risk transfer. Other ways of transferring risk include, for example, concluding long-term purchase contracts at predetermined prices (elimination of possible inflation risk by transferring it to the seller), concluding business contracts conditional on taking a minimum quantity of goods (reducing sales risk by transferring it to the customer), leasing (transfer of financial risk, which is associated with the ownership of the item, from the selling entity to the leasing company) or the purchase of short-term receivables, so-called factoring (transfer of the risk of non-payment of receivables from the supplier to the factoring company).

Risk Avoidance is the last legitimate risk management option for not performing an activity. However, this is a negative rather than a positive approach, which is completely unsatisfactory for addressing many risks. This approach is recommended only in extreme cases, i.e. if the probability of occurrence and severity of the impact of the threat are so high that the given level of risk cannot be accepted (e.g. an unprocessed business plan for which the risk of failure is disproportionately high).

The first activity of the risk management subprocess is the **selection of options**. When selecting the most appropriate risk management option, we should constantly monitor the balance between costs, implementation efforts, and benefits achieved with respect to legal and other requirements, social responsibility, and environmental protection. Many risk management options may be considered applicable either individually or in combination, and an organization may benefit from implementing a combination of risk management options. In general, however, it is difficult to recommend an optimal solution, which is always a reflection of a specific situation. However, there are some guidelines for selecting the most acceptable risk management options, which are based on the probability of occurrence and severity of the impact of the threat (Table 4).

	High probability	**Low probability**
Impact severity high	risk avoidance risk reduction (D is from 3 to 5)	risk transfer
Impact severity low	risk reduction risk retention (D is from 1 to 3)	risk retention

Table 4: Recommended principles for the selection of risk management options (adapted from Smejkal and Rais, 2009)

Legend:

D – severity of the impact

P – probability of occurrence

An example of a point range of impact severity and probability of occurrence is demonstrated using a semi-quantitative assessment method using a point scale from 1 to 5.

When choosing risk management options, we should consider the expectations and views of stakeholders and consult with them on the most appropriate ways. If certain risk management options appear to be equally effective, some options may be more acceptable to stakeholders than others. If the chosen risk management options may also have an effect on risks in another part of the organization, we should also involve these areas in decision-making. Resources for risk management are also an important factor in decision-making. If these resources are limited, when developing a management plan, we should clearly identify the priority order in which we recommend implementing the individual risk management options.

At the same time, it is important to take into account that risk management may in itself lead to secondary risks. A significant risk may be, for example, the ineffectiveness of the adopted security measures for risk management. Therefore, monitoring must be an integral part of the risk management plan, which provides assurance that the measures taken remain effective. Risk management can also cause secondary risks that must also be assessed, managed, monitored and reviewed. These secondary risks need to be included in the same risk management plan as the original risks (they should not be addressed separately as new risks) and the link between the two risk groups identified.

Managing entities and other stakeholders should be aware that, following the application of the chosen risk management options, it is necessary to re-identify the so-called residual risk and determine its type and extent. We should then document the residual risk and subject it to monitoring, review and, if necessary, further management.

As part of the second activity of the risk management subprocess, we will **implement risk management plans**. The aim of these plans is to document how the selected risk management options will be implemented. The information provided in such a plan includes the expected benefits, implementation measures and limitations, the persons responsible for approving and implementing the plan, the proposed activities, the monitoring and reporting requirements, the resource requirements and the timetable. The developed risk management plans are then discussed with relevant stakeholders and integrated into the organization's management processes. At the end of the risk management subprocess, it is necessary **to ensure the feasibility of selected security measures** and **to determine the acceptability of the residual risk**.

Process monitoring and review

Entry into the subprocess: Outputs of all subprocesses of the risk management process.

Subprocess activities:

1. Monitoring the risk management process
2. Review of the risk management process
3. Processing and transmission of results

Subprocess output: Records of the risk management process in the organization and documents for its updating.

Process monitoring and review should be considered an integral part of the risk management process. As in other stages of the process, it is appropriate to clearly define the responsibility. Process monitoring and review should cover all aspects of the risk management process, in order to analyze and learn from events, changes and trends, to detect changes in external and internal contexts (including changes in risks themselves that may necessarily require a review of the management subprocess and re-prioritization), to ensure that risk control and risk management measures are effective in both the design and implementation phases and to identify emerging risks. We can carry out monitoring and review in the form of constant supervision, regular inspections or one-off special-purpose inspections. The results of monitoring and review need to be properly recorded and communicated to internal and external stakeholders. At the same time, they will be used as input to review the risk management framework.

An essential part of monitoring the risk management process is its continuous recording. Evidence of the implementation of individual activities of the risk management process must always be properly traceable. As part of the risk management process, the records provide us with a basis not only for improving methods and tools, but also for the entire process. All decisions taken in relation to records should take into account the benefits for re-use of information for management purposes, the costs and efforts associated with creating and maintaining records, the legal and operational requirements for records, the way records are stored and accessed (e.g., storage media), the validity period of the records and the level of sensitivity of the information.

Summary

The general approach to risk management provides the organization with guidelines for implementing the basic elements of risk management in a clear and reliable manner in any scope and context.Each specific branch of safety engineering or the way in which risk management is applied brings with it individual needs, individual risk perceptions and the resulting differences of opinion when defining criteria for risk assessment.

The risk management process must be an integral part of the organization's management, it must be embedded in the culture and practice of the organization and it must be adapted to its processes.The risk management process consists of five basic sub-processes, which are communicationand consultation, context definition, risk assessment (includes risk identification, analysis and assessment), risk management and process monitoring and review.

In conclusion, it is necessary to draw attention to the fact that through the comprehensive implementation of the risk management process, organizations will achieve a significant increase in the safety of existing processes at all levels. Such organizations also prevent inefficient risk management, which is characterized by many serious shortcomings, such as context-free risk management, inefficient risk identification and risk factors, overly general risk definition,non-involvement of internal and external stakeholders, r discontinuity of the whole process.

Reference

AXELOS LIMITED, ed., 2017. Managing successful projects with PRINCE2. 6th edition. London Norwich: TSO. ISBN 978-0-11-331533-8.

DITTMANN, K., DIRBANIS K. Project Management (IPMA®), Haufe-Lexware, 2023, ID: 42533792

DOLEŽAL, J. Projektový management: komplexně, prakticky a podle světových standardů. Praha: Grada Publishing, 2016. Expert (Grada). ISBN 978-80-247-5620-2.

MÁCHAL, P., KOPEČKOVÁ M., PRESOVÁ R. IPMA, PMI, PRINCE2. Praha: Grada, 2015. Manažer. ISBN 978-80-247-5321-8.

SMEJKAL, V. RAIS, K. Řízení rizik ve firmách a jiných organizacích. 3. vyd. Praha: Grada Publishing, 2009. ISBN 978-80-247-3051-6.

TICHÝ, MILÍK. Ovládání rizika. Analýza a management. 1. vyd. Praha: C. H. Beck, 2006. ISBN 80-7179-415-5.