Katarina Buganová[1]

Katarina Hollá[2]

ENTERPRISE RISK MANAGEMENT FOR BUSINESS RESILIENCE

Abstract: The turbulent development of the global entrepreneurial environment brings a lot of aspects that force the managers to think about the negative impacts of their everyday decision-making. The erroneous decisions affect not only the stakeholders but also the further development of the company. Therefore the sustainable growth of the company assumes that the company managers are able to anticipate the potential risks and manage changes and in this way to prevent the possible crisis. Risk management provides guideline and methods how to facilitate decision-making with a focus on anticipating what can happen, why and how it can affect various objectives.

Key words: risk, risk management, resilience, enterprise, process

[1] Assoc. Prof. Katarína Buganová, PhD., Faculty of Security Engineering, University of Zilina, 1. mája 32, 010 26 Žilina, katarina.buganova@fbi.uniza.sk

[2] Ing. Katarína Hollá, PhD., Faculty of Security Engineering, University of Zilina, 1. mája 32, 010 26 Žilina, katarina.holla@fbi.uniza.sk

1. ENTERPRISE RISK MANAGEMENT FOR BUSINESS RESILIENCE

Enterprise risk management for increase the resiliency of businesses in the face of risk events

The success of enterprises depends on their ability to adapt to varying conditions and unstable conditions in business environment where they do their business. Risks arising from the instability of the business environment represent potential sources of crises for enterprises that often lead to the destruction of the business. The need to actively manage risks is based on the fact that a large number of enterprises has ceased during the first year since the establishment of the business. Underestimation, mismanagement, or ignoring business risks is the way to decline, and therefore, it is necessary to choose the right form of risk management. The big problem, considering enterprises, is often the lack of knowledge and experience of owners and managers in the field of risk management.

Risk management provides guideline and methods how to facilitate decision-making with a focus on anticipating what can happen, why and how it can affect various objectives. Implementation of risk management is carried out by systematic applying of policies, practices and resources to assessment, management and control of risk, focusing on the security of business continuity, in particular orientation on the achievement of business objectives. Risk management in enterprises should be implemented as an integrated system with clearly defined objectives, transparent structure and given procedures.

In the area of risk management, the resilience collaborates with business units to identify, review and propose actions and mitigation plans to address risks arising from business activities. The greater visibility of this work, coupled with the wide spectrum of activities it covers, has strengthened ability to manage risk and making enterprises a more resilient business [7].

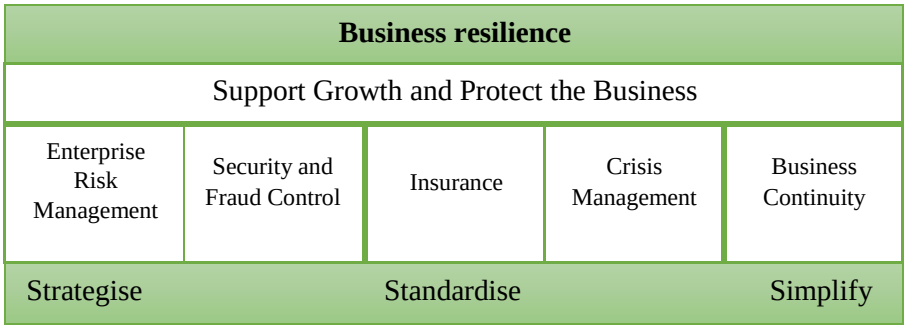

Figure 1 – Scope of the business resilience [7]

Risk management thus represents rational behaviour in risk situations in order to protect and improve current and future assets of the company through the systematic integration of risk into key management decisions. Risk management cannot operate in

isolation, detached from the corporate events in enterprises. It must be integrated into the system and respected for all subsystems in the company.

Risk management system is based on the fact that the risks (including their mutual links and interactions) are identified continuously, holistically proactive and systematically in the organization.

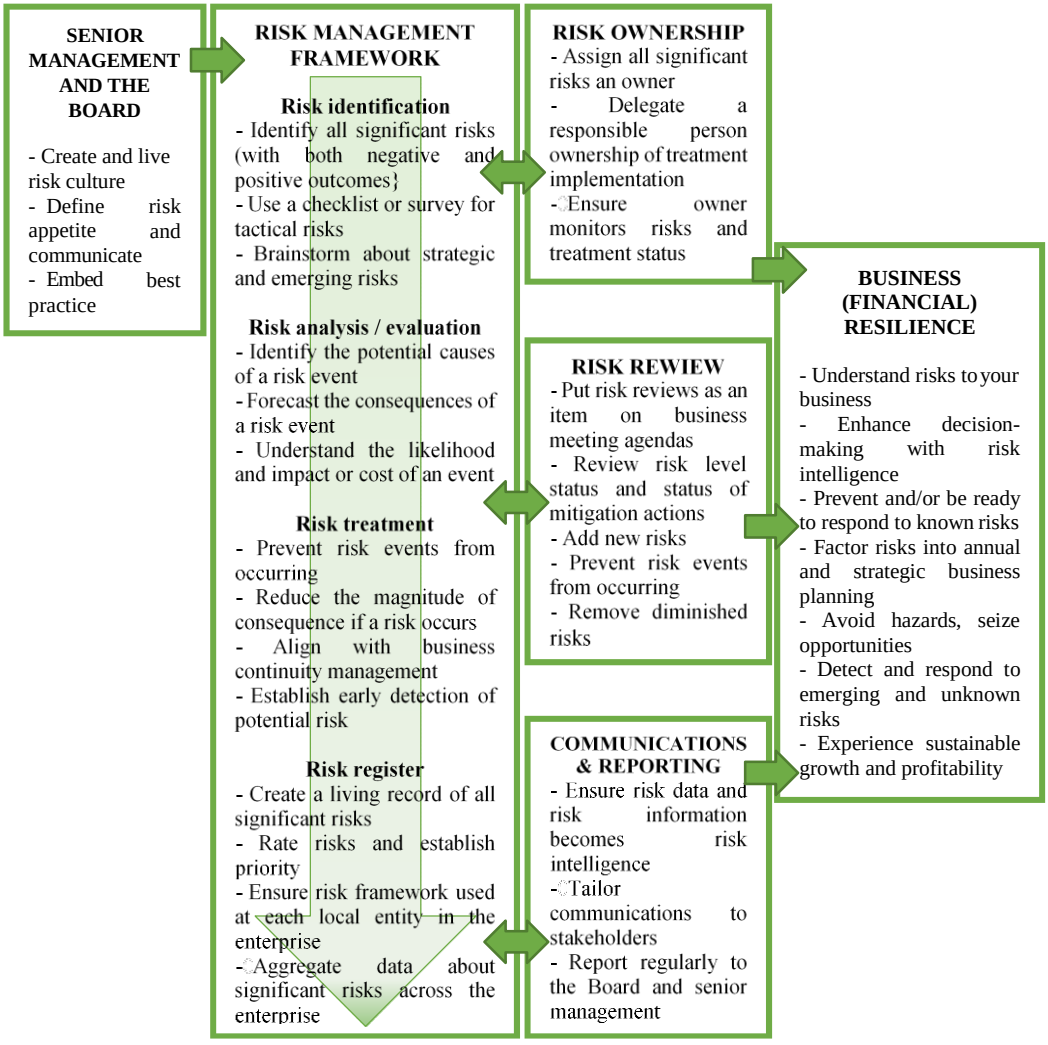

Figure 2 – Enterprise Risk Management (ERM) for Business Resilience [3]

Enterprise risk management (Fig. 2) process is enhanced to improve understanding of risks and opportunities and adapt business response based on experience and changing circumstances. Work teams utilise internal and external risk radar to detect changes in operating environment, which allows to work proactively to minimise exposures and leverage opportunities. This also gives enterprise the ability to respond rapidly and decisively to an emerging crisis [7].

The introduction of a risk management system in enterprises contributes to the maintenance or growth of enterprise value for its owners. It leads to higher quality of strategic management, greater stability, and faster responses to changing market conditions and to reduce probabilities of mistakes, errors and frauds.

Risk management process in enterprise

Risk management process [4] is the systematic application of policy management, procedures and practices in communication, consultation, establishing the context, identification, analysis, evaluation, processing, monitoring and review of risk (ISO 31000:2009 Risk management - Principles and guidelines).

Establishing the context

In the phase establishing the context, or recognition of context, there is defined the relationship between the organization and its environment, thus, identify strengths and weaknesses and the opportunities and threats. It is also necessary to assess the ability of the enterprise following the objectives, intentions and strategies.

In the phase of establishing the context, it is necessary to [6]:

- Define external links of risk management on the environment of organization (for example, in relation to external political, economic and social, technical and cultural environment, opportunities and threats, etc.)
- Define internal links of risk management within the company (for example, in relation to corporate culture, organizational structure, use of resources, objectives, strategies, etc.)
- Specify structure and internal risk management framework, defining objectives, strategy, content and parameters of company activities, which the process of risk management is applied to. Define the roles and responsibilities of individual organizational components of company within the risk management system.
- Establish criteria for the assessment of level of the risk in the company.

The most commonly used methods and techniques of analysis of external and internal environment usable also for SMEs are presented in Tab. 1.

Table 1- Selected methods and techniques of analysis of external and internal environment of the company [9]

Methods and techniques of analysis of external and internal environment of the enterprise	
Analysis of external Environment	STEP analysis (PESTLE analysis), Porter's five forces model, 4C method, or 7C method, analysis of stakeholders and other.
Analysis of internal environment	analysis of resources, VRIO analysis, analysis of internal capabilities profile, analysis of vulnerability, benchmarking, financial analysis, analysis of value chain, 7S method so called McKinsey analysis, Mallyova analysis of the internal environment and other.
Analysis of external and internal environment	SWOT analysis, SPACE technology, BCG Portfolio matrix, GE Portfolio matrix and other.

The structure of the risk management process will vary depending on the needs of small and medium-sized enterprises, character of the risks and subject of business. A significant risk for some small and medium-sized enterprises is the failure in achieving strategic, project or specific objectives, while the risks affect the fulfilment of the contractual obligations, reliability, trust and value of the company.

Establishing the criteria for risk assessment is the final step in the phase of the establishment of the context in the risk management process. It represents the criteria processing in comparison with which the level of risk will be assessed. Further, there are elaborated and specified risks after identification and they must comply with the type of risk and the way of the expression of the level of risk.

Establishing the context is the initial phase of identifying risks, therefore, it is necessary to pay sufficient attention to the choice and accuracy of the analysis applied. Inaccuracies or overlooked weaknesses, or threats may not be included in the catalogue of risk, so they do not get into the risk assessment, which may cause big problems for SMEs (in the event of such a risk, which it will not be ready for).

Risk assessment

The standard ISO 31000:2009 tells about risk assessment as a summary process of identification, analysing and risk assessing.

Risk assessment in small and medium-sized enterprises has great importance, because if the enterprise does not know or is unable to name and evaluate their risks, it exposes itself, their employees, customers and partners at risk of failure, or losses in various forms. The methods used in various phases (identification, analysis, evaluation) are usually useful at several phases associated in the risk assessment process and they cannot be completely separated.

Risk identification

According to ISO Guide 73:2009, risk identification represents process of finding, recognizing and describing risks.

The objective is to identify and define the key risks at all levels of management. Top management focuses mainly on significant market changes, customers, competitors, legislation etc. Executive management focuses on the risks of internal environment and business processes. Identifying the risk (factors, or risk sources) must be approached methodically in order to analyse all relevant business activities and identified risks arising from them [2].

The phase of identification is based mainly on knowledge, experience and intuition of managers and has a significantly creative character. When identifying, it is important to assess the reliability of information sources used, the need to obtain additional information, appropriateness of the choice of persons engaged in the identification, completeness of the list of identified risk sources etc. [10].

Potential risks that are not identified in this phase, are excluded from further analysis, therefore, risk identification has great importance in the process of risk management in the company. The result is a written list of potential risks – the risk catalogue.

Risk catalogues provide an overview of the risks (risk sources), or enterprise risk activities. Establishment of a catalogue reduces the risk that there will be overlooked of certain risks. Description of the risk should be part of the catalogue, i.e. word risk characterization.

Overview of recommended methods and techniques for risk identification [9]:

- Methods and techniques of environment analysis, e.g. vulnerability analysis, financial analysis, SWOT analysis etc.
- Methods and techniques for obtaining information, e.g. brainstorming, Delphi technique, nominal group technique, a structured talks and discussion with experts, questionnaires, security audits etc.
- Structured instruments, e.g. flowcharts, system analysis, case studies, modelling, affinity diagrams, analysis of causes and effects, mind maps etc.
- Risk catalogues, or risk registers, lists of risk. Provide exhaustive overview about potential risk factors, or company risks or their activities – control lists and checking tables etc.
- Clearly defined formal description of situations. Uses for the identification of risk at a strategic level and to define general processes. The objective is to describe the situations and say "What happens if".
- Combined sources of information. Applies mostly in situations with limited resources, or if it is necessary to increase the efficiency of outcomes.
- Multi-level identification. Implements in a number of consecutive steps.

A detailed overview of the internal and external factors of the enterprise such as risk resources can be obtained based on the conclusions from the analysis of the current state of enterprise, which is realized in the phase of establishing the context. This phase of the risk management process enables the identification of risk situations that could cause serious economic problems, or threaten its very existence in the future. Besides the negative factors, the company obtain an overview of the possible opportunities that may affect its future development.

Identification of risk is not a one-time matter, but an activity that is carried by purpose periodically or continuously. There are used monitoring systems and early warning systems, which, on the basis of selected indicators, regularly monitor the development of selected risk, and in case of exceeding set limits, they warn responsible persons of an increased value.

Risk analysis

Risk analysis is a process aimed at the basis of the risk and determines risk level [4].

Risk analysis is based on the output of phase of identifying risks and is based on improving the understanding of risk. Approaches to risk analysis vary according to the standards and approaches to risk management. It often links with the risk assessment. When analysing the risk, there are assessed sources of risk, existing measures and analysed risks in terms of consequences. There is taken into account a set of potential consequences and possibilities that these effects occur. Consequence and probability are combined to give the level of risk, or rate of risks (significance, importance).

Risk analysis can be performed at different levels of detail depending on the specific risk, analysis purposes and available sources of information.

The analysis can take place in two stages:

1. The first phase processes preliminary analysis to eliminate similar risks or risks with very little impact from the list of identified risks. The risks excluded are necessary to register further in order to demonstrate the completeness of risk analysis. It also provides basis for subsequent decisions about the method of risk analysis itself of the company.

2. The second phase processes detailed analysis of risk using risk analysis methods (qualitative, semi-quantitative and quantitative). If the combination of the methods used, it would be best, but time consuming and expensive.

According to the depth of processing analysis, available information and the purpose for which the output of the risk analysis has to be used, it is therefore possible to apply qualitative, semi-quantitative and quantitative analysis, and combinations thereof. Qualitative or semi-quantitative analysis is mostly suitable for SMEs, which allows obtaining a general estimate of the level of risk. It is possible to make more specific quantitative analysis for selected types of risks.

In terms of orientation, risk analysis can be classified as [8]:

- Analysis of the effectiveness of existing controls - determines if current control monitors the treatment of risks to the necessary level and efficiency of operating factors.
- Analysis of consequences - determines class and type of impact, if a particular event, situation or circumstance occurs.
- Analysis of the probability of occurrence - to estimate the probability of risk, there can be used extrapolation techniques, predictive technology and expert evaluation.
- Analysis of uncertainty and sensitivity - assesses the uncertainty associated with the data, methods and models used by the process of identification and risk analysis.

Depending upon the amount of factors used in the calculation of the degree of risk, it is possible to quantify the level of risk as follows.

The risk can be expressed by the following relationships:

Risk = probability of negative phenomenon x losses in the number of negative phenomena.

Risk = probability of negative phenomenon, or threat x consequence of the creation of a negative phenomenon (in measurable units, e.g. monetary).

Risk = danger (threat) / preventive measures (protection).

Level of risk (R) is a numeric value or a function that describes the relationship of probability of occurrence (development) of negative phenomenon and severity of the consequences of negative phenomenon that may arise as a result of the risks involved [66].

Mathematical formulation of risk is based on a number of factors entering the calculation of the degree of risk.

(1)

( ) (2)

where:
P – expresses the probability of a negative phenomenon,
N – expresses the seriousness of its consequences,
V – expresses the significance of the threat represented by the risk involved,
S – expresses different types of consequences, or scenarios for the origin and course of negative phenomenon.

$$R = \sum_{i}^{n} Pix \sum_{i}^{n} Ni \tag{3}$$

where: i, j - are indexes related to potential i – negative phenomenon and consequence for i = 1, ... n.

Another way is considering the vulnerability of the company and the value of distressed assets:

$$R = P \times Z \times A \tag{4}$$

where:
A – represents the value of assets = brand, customers, contracts, equipment, something that represents value for the enterprise to be protected,
Z – vulnerability of the company, i.e. the set of circumstances that allow negative phenomenon affecting assets, e.g. departure of chief executive, inadequate security system, absence of risk management etc.

The combination of these parameters does not mean in practice only mathematical operation of the product (it is so called Cartesian product, an ordered pair of elements). In the case of Cartesian product, besides P and N, it is not possible to take into account time exposure and the possibility of prevention, or protective resources depending on the available information. This approach takes into account that, for example, if the value of the probability and consequences will take values 1 and 3, then:

$$\textit{When } P = 1 \textit{ and } N = 3, \textit{ then } R = P \times N = 3$$

$$\textit{When } P = 3 \textit{ and } N = 1, \textit{ then } R = P \times N = 3$$

It a difference whether there is a high probability of negative phenomenon with negligible consequences on the enterprise (in this case it is not necessary to perform risk reduction measures) or there are devastating consequences of negative event with a low value of probability (in this case it is necessary to insure, against such risks) [9]. Such understanding of the risks enables to transform it into a series of measurable categories. The term "level of risk" often used is not substantively different from the concept of risk, but highlights that it is a measurable quantity.

There are mostly two ways to determine the significance of risk in the literature (levels, degree): sensitivity analysis and expert evaluation. The basis of expert evaluation of risk significance using risk assessment matrices lies in the fact that the significance is assessed in terms of the probability of risk occurrence and intensity of positive / negative effects on the company.

It is possible to several methods and tool when analysing risk in small and medium-sized enterprises (SME). The use of these methods in the SME also depends on whether they are applied at the strategic, or operational level of the company, what expertise and experience, resources available for risk reduction management has etc.

Table 3- Selected methods and techniques for risk analysis [9]

Methods and techniques for risk analysis	
Scoring method (risk assessment matrix)	*Based on qualified estimate of assessors, who specify the probability of the risk occurrence and intensity of adverse effects. Combination of these two parameters determine the value of risk (level of severity).*
Scoring method (using real numerical values)	*Uses quantitative probability detection of the occurrence of risk (e.g. 1 injury per 100 000 workers, etc.) and consequences (e.g. value in €, environmental damage, etc.) based on actual values over time, but also expert estimate of these parameters, if it is not possible to determine quantitatively their value.*
Sensitivity analysis	*Based on explicit modelling of the impact of risk on the effects of the business plan, expressed by evaluation criterion, using the amount of expected profits. The basis of this method is the recognition of sensitivity of the selected criteria (e.g. profit) of possible changes in levels of risk factors that affect this criterion.*
Network diagrams	*Have an important role, particularly in project management as a tool for complete and clear registration of large amount of information needed for management. It is possible to identify easily the necessary resources and time for individual phases and the project as a whole from the network graph. The methods of network analysis include the method* ***CPM – Critical Path Method****,* ***ADM - Arrow Diagramming Method*** *and others.*
Statistical methods	*Used to measure the absolute level of risk by using basic statistical characteristics:* ***variance, standard deviation and coefficient of variation.*** *These quantities of levels of risk characterize variability criteria (e.g. profit, return on equity), to which the risk entrepreneurial project (activity) determines [20].*
Simulation models	*Used when the problem is too complex for the use of other methods of risk assessment or there is a large number of risk factors. There is expected the use of computer programmes [69], for example,* ***Monte Carlo simulation.***
Graphical methods	*Useful for determining and displaying the consequences (impact o effects) of risk variants with respect to the selected evaluation criteria. They are particularly* ***decision matrix, decision trees, and probabilistic trees (tree of significance).***
Deterministic, or probabilistic analysis	*Adoption of the decision is in the context with the above approaches associated with the application of the following decision criteria:* ***maximax, maximin, expected monetary value – EMV, expected opportunity loss - EOL*** *and others.*
Value at risk - VaR	*VaR reflects a loss for a defined time horizon and a given value of confidence expressed by coefficient. VaR does not represent a worst case scenario and either cumulative loss of company. VaR is a complement to other methods expressing the level of risk and risk management policy of the company.*

From the perspective of management the methods and tools mentioned are used not only for the needs of risk management, but also in standard management practice.

Risk evaluation

Risk evaluation is the process of comparing the results of the risk analysis with risk criteria to determine whether the risk and its size are acceptable or can be tolerated [4].

This phase is often identified, or connected in terms of content with the phase of risk analysis. In this case, the level of risk is determined by means of selected methods in the evaluation phase. The second approach, which is also mentioned in standard ISO 31000:2009 describes this phase as a process aimed at prioritizing risks based on the risk evaluated in the previous phase of risk analysis. The risk evaluation in this sense is identical with the concept of the evaluation of risk.

After completing the risk analysis process, it is essential to compare the estimated risks with predetermined criteria. Therefore, the evaluation of risks is a tool to assess the severity of the risks to the enterprise and whether it is necessary to accept the risk or implement necessary measures [1].

It is very important to determine limits of acceptability, which is usually influenced by subjective opinions. It is recommended to use collective decision-making when determining.

Acceptability of risk should be based on generally accepted principles such as ALARP principle (As Low as Reasonable Practicable), which is also part of the ISO 31010:2009.

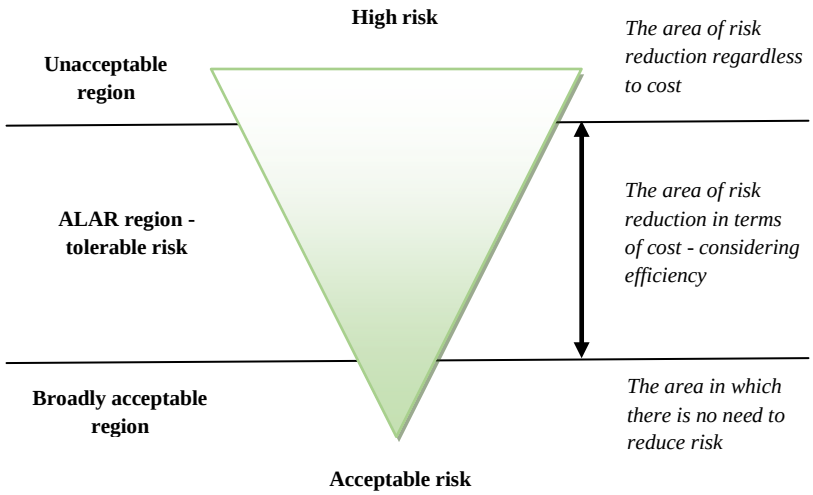

Fig. 3. Level of risk according to the ALARP principle [5]

ALARP (Fig. 3) is the principle of reducing risks to as low as is reasonably practicable, that the cost of further risk reduction would be disproportionate to the benefits of the implementation of these measures. The higher the level of risk, the more you can expect that more effort to reduce it is made. According to the ALARP principle, the risks may be divided into three regions in terms of the economic acceptability [5]:

1. **Region (high)** above which the risks are unacceptable and must not occur except in emergency situations.

2. **Medium region** - the area between the boundaries (Fig. 3.3), where there are risks that already cannot be reduced by standard approaches. Risks need to be kept as low as possible in two ways:

- at the bottom that is close (acceptable) negligible risks, it is possible to follow strictly objective cost-benefit analysis, i.e. select the most effective solution and if the costs for risk management are higher than the revenues on the asset, the risk is not treated at all,
- at the top, which is close to intolerable risks, it is assumed that the risk management measures will be implemented, even if costs incurred exceed revenues.

3. **Region (low),** below which risks are acceptable, there is no need to intervene actively and the risk can be just monitored.

The difference between tolerating risk and its acceptance lies in the fact that if the risk is tolerated, it needs to control it and reduce as much as possible (not ignored). If the risk is tolerable, it can be adopted in the form in which it exists.

Analysis of risk and criteria, which are compared in the evaluation of risks, should be based on the same basis. Qualitative evaluation assumes a qualitative comparison of the region of risk with the qualitative criteria.

The quantitative evaluation compares the numerical value of the risk with criterion expressed by particular number, e.g. frequency or financial value. Steps of risk evaluation are:

1. Setting the region of tolerance (appropriateness of the costs, delays etc.).

2. Assignment of the probability of occurrence and consequences to particular risks (cost, loss, reduced profitability, loss of time and loss of quality). This step is based on the risk analysis phase.

3. Prioritization of risk (based on the region of tolerance, potential costs of risk and probability that the risk will occur (becomes a reality). If costs of risk exceed tolerance region and it is highly likely that the risk will occur – risk will be a high priority solutions).

Boundaries between the low risks with low priority solutions, medium and large risks with high priority solutions are determined by enterprise based on experience and the level

of acceptability of risk. There is used Pareto principle (80:20) in the risk management of enterprises and projects, i.e. 20% of the most significant risks will bring 80% of losses, or costs. These risks are the highest priority for removal.

The most common form of risk evaluation are risk evaluation matrix (Risk matrix), or opportunities. The base is expert risk evaluation by workers (external consultants, experts) who have the necessary knowledge and experience. A certain risk is the more important, what is likely to occur and the higher the intensity of the impact (consequences) of this risk.

In the context of risk evaluation and subsequent measures on risk management, there are recognized the following types of risk [9]:

- Inherent risk – level of risk if there are not implemented any measures for risk treatment in the company (e.g. before the introduction of risk management, or early phase in the risk assessment). Inherent risk is every risk associated with the activity of the enterprise itself.
- Residual risk – current level of recorded risk (taking into account the measures implemented). Residual risk is the risk that is left after implementation of measures to manage risk. If the residual risk is higher than the target risk, there are proposed new forms of a reduction to an acceptable level.
- Target risk – a target state, which does not require any activities to address it because the risk is acceptable.

		Consequences (Intensity of the negative impacts)				
Probability		1	2	3	4	5
		Very small	**Small**	**Medium**	**High**	**Very high**
5	**Very high**					Inherent
4	**High**			Residual		risk
3	**Medium**			risk		
2	**Small**	Target				
1	**Very small**	risk				

Fig. 4 Risk matrix – possible movements in the risk evaluation [9]

When evaluating inherent risk, any risk reduction measures that were implemented in the company are not taken into account. Residual risk takes into account the measures for treatment of risk, already introduced, but not prepared, or planned. The transfer of risk in the matrix from inherent to residual is implemented on the basis of a proposal from the risk owner, after the implementation of measures to cope with risk and evaluating their effectiveness (success). The same shall apply for the transfer of residual risks to the target group (Fig. 4).

A great impact on the establishment of boundaries in determining the level of risk has attitude (relation) of manager (management, company) to risk. This attitude is influenced by their personal characteristics and experiences of the past. It is also influenced by the enterprise management system, for example, willingness to risk stimulates good motivational system, tolerance of minor failures etc.

Managers may have:

- **risk aversion,** try to avoid risky activities and look up low-risk projects with high probability lead to the achievement of outcomes that are acceptable to them,
- **risk taking,** in this case, on the contrary, look up risky activities and projects that are likely to deliver very good results, but are associated with a great risk of negative impacts, or losses,
- **neutral attitude to risk** (risk neutrality), when the aversion and inclination to risk are in balance.

Other indicators affecting risk evaluation to be taken into account already in the implementation of risk management are risk capacity and the size of tolerated risk:

- **Risk capacity** is usually expressed as the highest financial loss that the company is able to survive, i.e. the size of such losses, which still does not affect its existence. The amount of risk capacity depends primarily on the size of the capital of the company, its structure and ability to obtain additional sources of funding. This value must never be exceeded when determining the amount of acceptable risk (losses).
- **Risk appetite** (size of tolerated risk) represents the total amount of risk in which there must be achieved the defined objective (profit) of the company. It is specified in the development of the strategy and risk reduction measures must be set so as not exceeded. It depends on the requirements and expectations of stakeholders (shareholders, creditors, etc.) and the attitude to risk management.

The output of the risk assessment process is a complete catalogue risk with the priorities to manage the risk. Risk catalogue should include all relevant information about the risks in the company and each risk should have its own card risks including the details of the status of risk throughout the risk assessment process. If risks classified belong into the category of low or acceptable risk, they can be accepted, monitored and reviewed periodically to make sure that remain acceptable. If the risks belong into a higher risk category, they should be given more attention and apply the necessary measures.

Risk treatment

Risk treatment is the process of selecting measures to risk management, assessment, preparing risk treatment plans and their implementation. In the literature, this process can also be called risk management, risk solutions, risk management, risk treatment, control etc.

This phase follows risk evaluation. The efficiency of measures is expressed in terms with which the risk will be eliminated or reduced by introducing the proposed control measure. The costs of introducing measures should be quantified as accurately as possible, because they are a basic measure to assess the financial performance and efficiency of measures. Furthermore, it is necessary to estimate expected losses, if there have been no steps to reduce risk. In the vast majority, we cannot talk about minimizing business risk, because the higher the risk, the higher the possibility of potential profit and vice versa, but its reduction to a certain economically acceptable level. Therefore, the business activity remains, to some extent, still risky.

Basic procedures and methods of risk treatment are as follows:

- **Risk retention** – adoption, or risk acceptance is the most common method of risk management. Conscious risk retention occurs when, after identifying, there are not made any measures for its management. All retained risks need to be monitored. If the risk is not recognized, then it comes to unconscious risk retention. There can be also included risk preservation in this category due to its low importance and high costs to remove them. This also applies to any residual risks and risks that have not been identified for some reason [8].
- Risk reduction can be realized in two ways. Offensive approach gives evidence of reducing the probability of negative risk occurrence and is based on the implementation of preventive measures. Measures should be specified for specific risks, which can affect the occurrence of events or factors having an impact on company objectives. Defensive approach consists of reducing the severity of the risk consequences and measures ex post. There are applied measures affecting the impact of the risks, whose occurrence can not affect company objectives, for example, increase in prices of materials or energy.
- Risk transfer also represents defensive approach of risk management. Risk is transferred to another, economically powerful entity. The causes of such risks (e.g. elimination of competition by political or economic power) are not removed, but attention is paid to reducing the adverse consequences of risk. The most common forms of transfer are, e.g. insurance, long-term sales contracts, leasing, factoring, etc.
- Risk avoidance represents not to carry out given risk activity. It represents a rather negative approach to risk management; it can cause the occurrence of new risks, or result in the loss of opportunities. This approach is directly related to the company's willingness to take risks and recommended only in cases where the probability and severity of consequences of risks are so high that they are

unacceptable, for example, the business plan with a high risk of failure, security and criminal risks.

High probability	*Reduce the risk* *Accept the risk* *(risk retention)*	*Risk avoidance* *Risk reduction*
Low probability	*Risk acceptance* *(Risk retention)*	*Insurance*
	Low severity of consequences	**High severity of consequences**

Fig. 5 Recommended methods for general problem solving of risk in enterprise

In practice, the use of those approaches is not so clear; however, this classification can be used in the analysis phase of a specific risk and risk policy of the organization. Procedures for reducing business risk can be divided in to two groups, namely:

- Offensive procedures aimed at elimination or weakening of risk causes. The objective is to influence own risk causes in order to prevent future situations that are unfavourable for the company. Therefore, they are preventive measures.
- Defensive procedures aimed at reducing the adverse consequences of risk. These measures are aimed at reducing adverse impacts of the occurrence of certain risks. These measures, prepared only in the form of certain plans and implemented only in the event of risk occurrence, are referred to as corrective measures.

The measure chosen should be developed as a plan (scenario) of risk treatment. The plan should include responsibility for risk, schedule, expected result, funding, performance rate and review process to be used etc. If, after risk treatment, there appears residual risk, it must be considered, whether we accept it or repeat the whole process.

Monitoring and review

Risks and effectiveness of measures introduced must be monitored to ensure that changing circumstances do not change priority risks. Permanent monitoring is important that the management plan is still valid. Factors that may affect the probability of risk occurrence and consequences may change, as well as factors that affect the appropriateness of the measures of risk treatment or cost. Therefore, it is important to continuously and periodically update the data monitored.

System of monitoring and review is based on the risk register. Every risk that is considered critical should be recorded and the information about it should be delivered to competent persons. Instrument that records can be e.g. updated catalogue of risks, risk

card consisting of a set of standard monitoring data, risk report processed by the responsible worker to a certain date, etc. To inform the responsible managers there can develop so-called summary report on the risks. Review is based on the monitoring of the operation of the various phases of risk management in order to ensure the highest efficiency of the risk management process. There should be recorded assumptions, methods, data sources, analyses, results and reasons for the decision in each phase. This information will improve the clarity and readability of the risk management process and are the basis for monitoring and review.

Communication and consultation

Effective communication is important to ensure that those responsible for the introduction and implementation of risk management, as well as the persons, understand the basis of the decisions and the reasons for the need and importance of specific measures. The communication plan should be developed at the beginning of the risk management process.

Communication and consultation are a two-way dialogue between stakeholders, so-called "stakeholders". Consultations are important because each participant of risk management process can have his/her own experiences and other perception of risk, which may be hidden for the rest. The opinions of interested groups have a great influence on decision-making and overall success of the entire risk management process, therefore, it is important to identify perception of risk, record and include it in the decision-making process.

Communication and consultation help to determine the context in the process of risk management for the identification of a wide range of risks; they accumulate knowledge from different areas of expertise in risk analysis and risk assessment as well as approaches to risk treatment and monitoring.

2. QUESTIONS

1. How would you define Risk Management in the enterprise?
2. What are the benefits of risk management in company?
3. How do we identify risks?
4. Is risk management considered by management as an integral part of management and their responsibilities?
5. At what level are Serbian companies using risk management?

3. REFERENCES

[1] ARMS – *A risk management standard*. Published by AIRMIC, ALARM. 2002

[2] Buganová K. et al., *Risk management in Enterprise*. Žilina /Slovakia, EDIS, pp. 226, 2012

[3] *Enterprise Risk Management (ERM) for Business Resiliency*, (25/11/2017) Retrieved from https://risk.thomsonreuters.com/content/dam/openweb/documents/pdf/risk/infographic/erm-business-resiliency-infographic.pdf

[4] ISO 31000:2009 Risk management – Principles and guidelines.

[5] ISO 31010:2009 Risk management – Risk assessment techniques.

[6] Kafka T. *Pruvodce pro interní audit a risk management*, Praha. C. H. Beck 2009

[7] *Risk management* (25/11/2017) Retrieved from https://coca-colahellenic.com/media/2596/business-resilience.pdf

[8] Rybárová D., Grisáková N. *Podnikateľské riziko*, Bratislava: Iura Edition 2010.

[9] Simák, L, Buganová, K. et al. *Risk management of small and medium enterprises*, Germany: A&A Digitalprint GmbH, 2017

[10] Varcholová T., Dubovická L. *Nový manažment rizika.* Bratislava: Iura Edition 2008.