UNIVERSITY OF ŽILINA
Faculty of Security Engineering

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

Date: 3.- 8. 11. 2017

Knowledge FOr Resilient soCiEty

ENTERPRISE RISK MANAGEMENT FOR BUSINESS RESILIENCE

Author: Assoc. Prof. Katarína Buganová, PhD.
Author: Ing. Katarína Hollá, PhD.

Faculty of Security Engineering

- 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.
- 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.

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

- 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.

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

SCOPE OF THE BUSINESS RESILIENCE

Business resilience				
Support Growth and Protect the Business				
Enterprise Risk Management	Security and Fraud Control	Insurance	Crisis Management	Business Continuity
Strategise	Standardise			Simplify

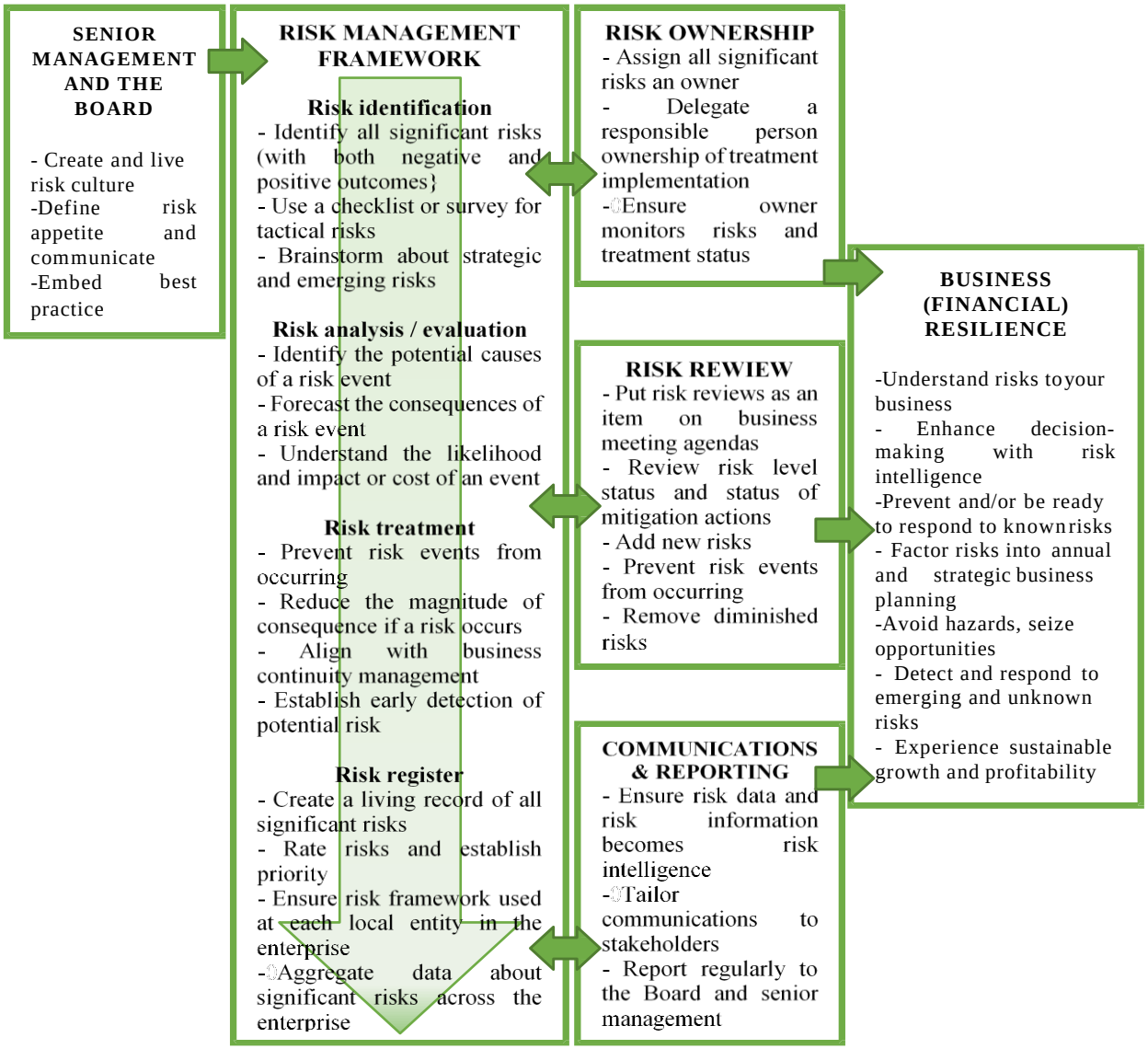
Co-funded by the
Erasmus+ Programme
of the European Union

RISK MANAGEMENT & BUSINESS RESILIENCE

- 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.

ENTERPRISE RISK MANAGEMENT FOR BUSINESS RESILIENCE



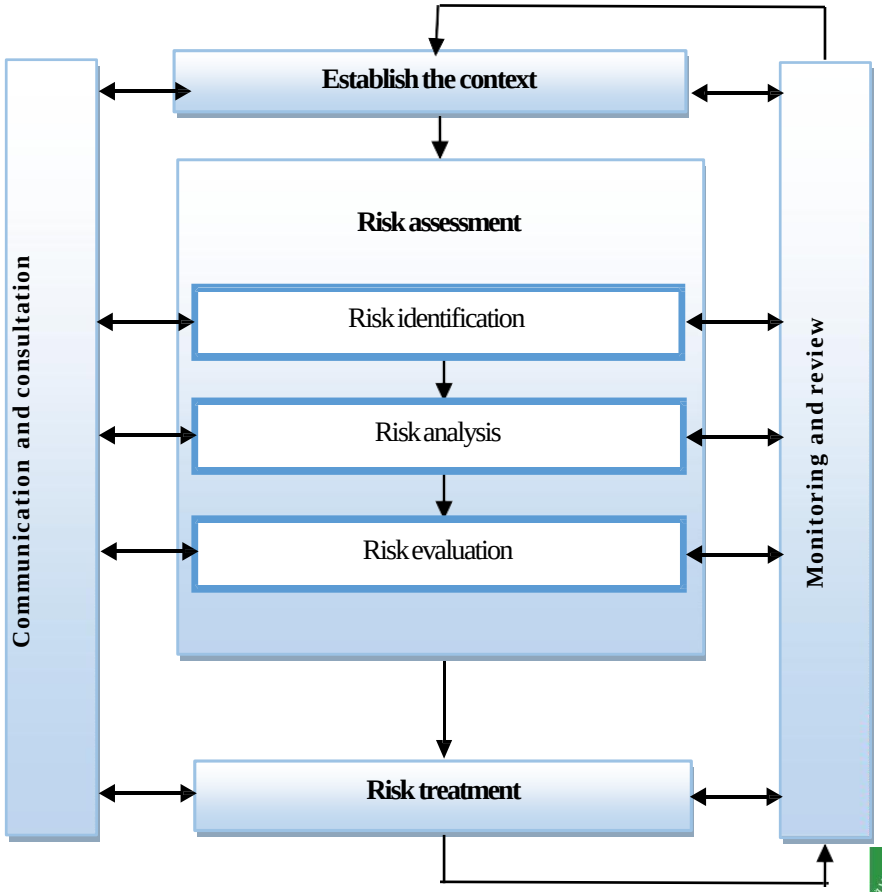
UNIVERSITY OF ŽILINA
Faculty of Security Engineering

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

RISK MANAGEMENT & BUSINESS RESILIENCE

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

RISK MANAGEMENT PROCESS IN THE ENTERPRISE



- **Risk management process** 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).

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

RISK MANAGEMENT PROCESS - Establishing the context

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

- 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.

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

Selected methods and techniques of analysis of external and internal environment of the company

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.

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

RISK MANAGEMENT PROCESS - Risk assessment

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

- Risk assessment in 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.

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

RISK MANAGEMENT PROCESS - Risk identification

- 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.
- The phase of identification is based mainly on knowledge, experience and intuition of managers and has a significantly creative character.
- 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.

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

Overview of recommended methods and techniques for risk identification

- *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* (registers) provide exhaustive overview about potential risk factors, or company risks or their activities – control lists and checking tables.
- *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.

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

RISK MANAGEMENT PROCESS - Risk analysis

- 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).
- 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.*

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

- **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.

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

- **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.

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

$$R = P \times N$$

$$R = f(P, N, V, S)$$

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.

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

$$R = P \times Z \times A$$

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.

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

Level of risk (R)

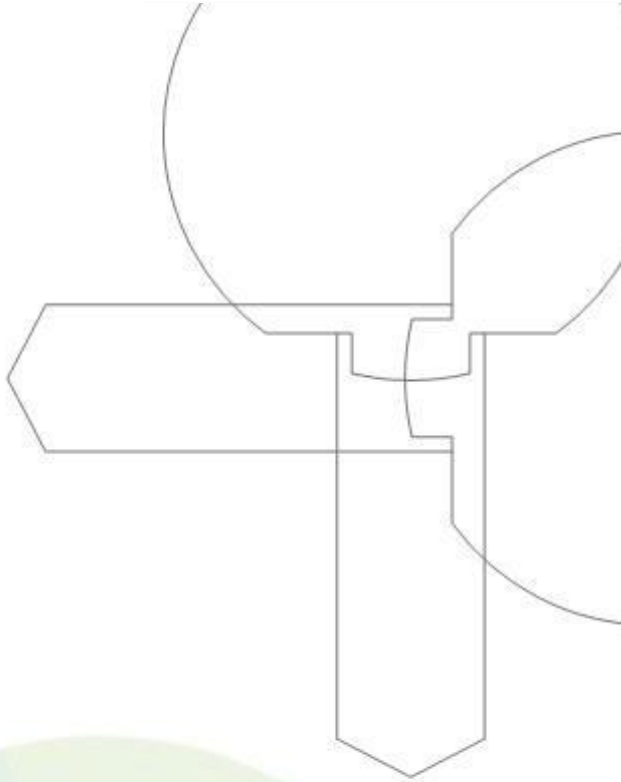
The combination of these parameters does not mean in practice only mathematical operation of the product (it is so called Cartesian product, an ordered pair of elements). In the case of Cartesian product, besides P and N, it is not possible to take into account time exposure and the possibility of prevention, 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:

When P = 1 and N = 3, then R = P x N = 3
When P = 3 and N = 1, then R = P x 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).

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 of 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.*

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



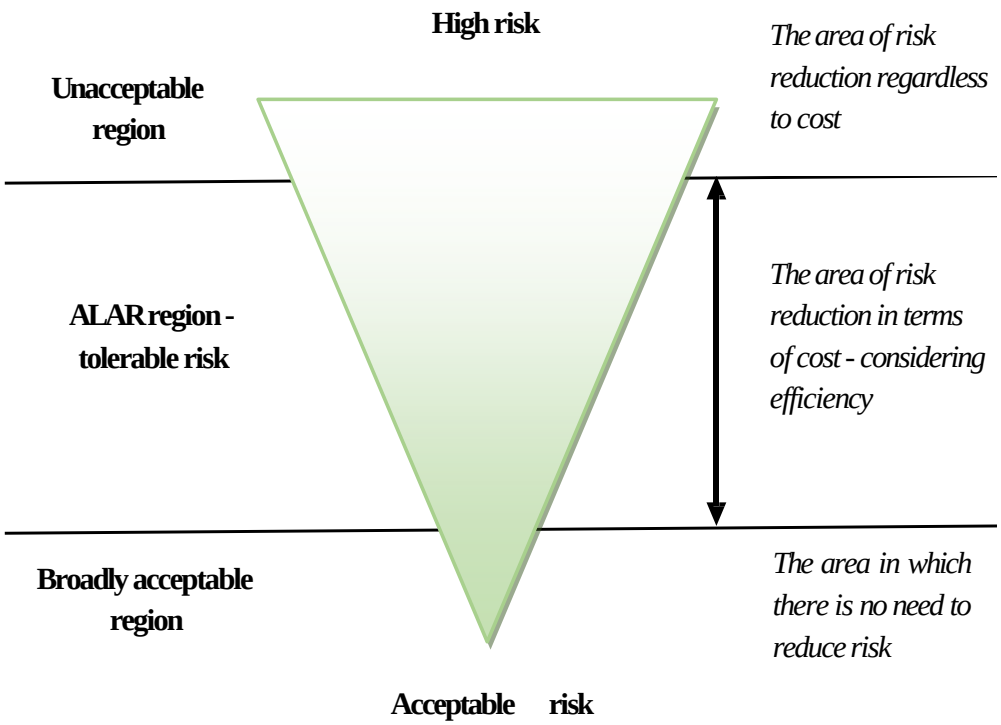
UNIVERSITY OF ŽILINA
Faculty of Security Engineering

RISK MANAGEMENT PROCESS - 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 .
- 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.
- 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.

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

Level of risk according to the ALARP principle



ALARP 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.

UNIVERSITY OF ŽILINA
Faculty of Security Engineering

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

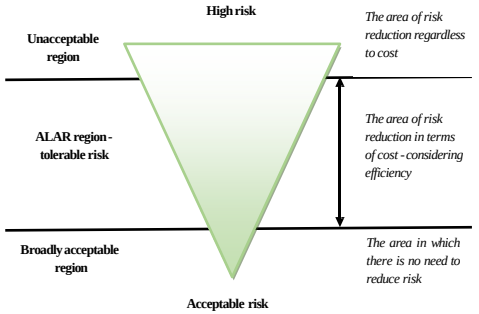
According to the ALARP principle, the risks may be divided into three regions in terms of the economic acceptability:

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, 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.



UNIVERSITY OF ŽILINA
Faculty of Security Engineering

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

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

		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				

Risk matrix

UNIVERSITY OF ŽILINA
Faculty of Security Engineering

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

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.

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

Risk capacity & Risk appetite

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.

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

RISK MANAGEMENT PROCESS - Risk treatment

- Risk treatment is the process of selecting measures to risk management, assessment, preparing risk treatment plans and their implementation.
- 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,
- attention is paid to redu
common forms of transfer
- **Risk avoidance** represe
the occurrence of new i
approach is recommended only in cases where the probability and severity of consequences of risks are so high that they are unacceptable, e.g. the business plan with a high risk of failure.

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**

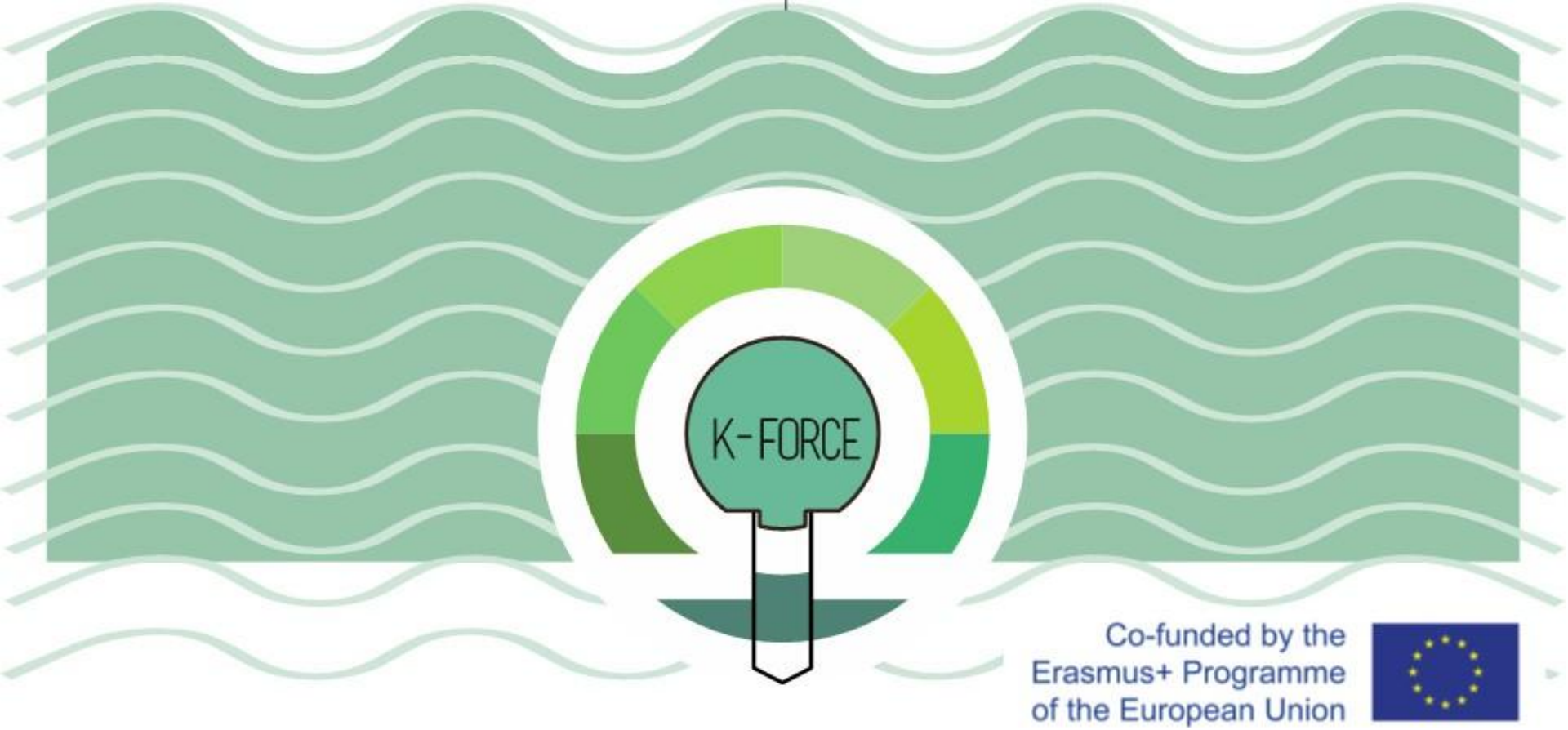
RISK MANAGEMENT PROCESS - Monitoring and review

- 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.
- 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.

RISK MANAGEMENT PROCESS - Communication and consultation

- *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.

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



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

Thank you
for your attention

Contact info about the presenter:
Assoc. Prof. Katarina Buganová (katarina.buganova@fbi.uniza.sk)
Ing. Katarína Hollá, PhD. (katarina.holla@fbi.uniza.sk)

Knowledge **FO**r **R**esilient so**C**i**E**ty