

Risk Management in the Higher Education Quality Insurance System

Živko Kondić, Željko Knok, Veljko Kondić, Sanja Brekalo

Abstract: Due to the factors that affect the results of work on a daily basis, higher education institutions, through their quality assurance systems, or their planning, must assess risks. In doing so, they must take into account all issues of the internal and external context as well as the needs and expectations of all stakeholders in higher education. The paper explains in an appropriate way the concept of risk as well as all the elements that determine it and their classification in the field of higher education. Subsequently, a possible approach to risk management is discussed, with an emphasis on clarifying the principles and the risk management process itself. Finally, the basics of practical application in risk identification, analysis, evaluation and treatment are outlined.

Keywords: opportunities; quality assurance; risk; risk management

1 INTRODUCTION

Throughout human history, man has lived and worked in an environment that has always been precarious. Risks have always been a constant companion for man. From prehistoric times people have lived in risky situations. The first risks were related to the inability to procure basic foodstuffs, protection from other species and other necessities for life. Human development has seen many lifestyle changes and the dangers around us. Our activities and lives have become more complex, and so have the risks. Today, we live in environments where exposure to risks is constant, such as traffic risks, food consumption risks, pollution risks, health risks, weather risks, theft risks, risks of various viruses, deadline risks, etc.

In a word, risks are an unavoidable and imminent in everyday life, whether in the private or business sphere. There is no absolute certainty in any business or activity, including in higher education. The only sure thing is that nothing in life and work is safe. There is always an aspect of "certain" uncertainty, risk that is taken or otherwise treated. Risk compromises and challenges goals and achievements, and therefore must be given a certain importance.

Many experts and scholars have discussed risks in an effort to come up with a definition of risk that would be acceptable in all fields of activity. Unfortunately, they have not been unable to fully agree. The reason lies in the fact that the risk is viewed as: "potential loss", "probability of loss", "uncertainty", "dispersion of real from expected results" or as "probability of an outcome that is not expected".

In addition, in all risk definitions, there are two common elements, uncertainty and loss. The significance of uncertainty in risk implies that the outcome of an event is always questionable. If there is a risk, then there are always two possible outcomes. If there is great certainty that the loss will occur, then there is no risk or its magnitude is insignificant. Likewise, if the outcome of an event is certain, there is no risk in that case. Risk is a combination of the likelihood and consequences of an adverse event [1, 2].

When it is said that risk is possible then it is implied that its probability of realization is between 0 and 1. This means that it is neither impossible nor safe to realize. An event can

be unrealizable (probability = 0), certain (probability = 1), or uncertain.

The word risk is derived from the ancient Greek word "rizko" which in translation means a danger to be avoided. Some associate the term risk with the old Italian word "risiko". The word risk itself is a little more difficult to understand, and very often, misused. In English, it is mostly used when talking about a chance or a gamble. The meaning of the word risk itself varies in function from the context in which it is used. It has mostly negative connotation. For example, one can rarely hear that there is a risk of winning the lottery, but it can often be heard that there is a risk of failing the exam. According to [3], risk is defined as the effect of uncertainty on targets, where the effect is considered to be deviation from the expected - positive or negative (Fig. 1).

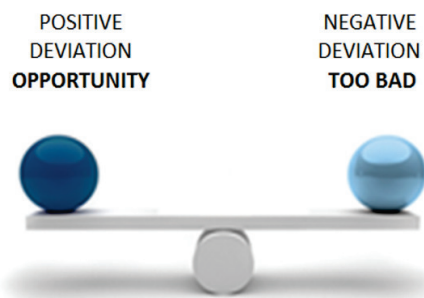


Figure 1 Effect of deviation from expected [4]

It can be simply said that risk represents the possibility of an event that will have consequences for the achievement of the goals. Unused opportunities or the opportunities for improving a business are also considered a risk. Accordingly, risks are potential adverse events that, for example, in higher education institutions may:

- compromise the achievement of strategic and operational goals, programs and projects, systems and activities;
- impair the quality of study;
- cause dissatisfaction of stakeholders in the processes;
- compromise the reputation of the institution and the confidence of citizens and future students in it;
- expose the institution to negative financial effects;

- compromise professionalism and appropriate (ethical) conduct in conducting business;
- result in misuse of funds, unauthorized use or misappropriation of property or information;
- adversely affect the institution's ability to manage the changed circumstances in a way to minimise or prevent their negative effects on the realization of the study.

As previously mentioned, the risk may be lower or higher, but it is always present in the processes. As such, it cannot be eliminated, but it can be controlled. This is an undesirable inevitability with which all organizations, including educational ones, coexist. The need for systematic risk management is necessary for survival and further development. If the risk is complex and uncontrollable, it triggers a crisis that erodes the institution at its root. The only way to completely avoid all the risks is not to work at all, which is not possible. Therefore, the risks are sought to be minimized by applying some of the techniques available for risk management. As quality assurance in higher education (QA) has become a daily occurrence at European and Croatian universities and colleges, [2, 5] it is necessary to initiate new support and management processes that address risks and opportunities through its activities.

2 DEFINITION OF BASIC TERMS

To understand the risk, one must also know its internal context, i.e. terms such as threat, vulnerability, consequence, risk criteria and risk owner.

2.1 Threat

Threat is defined as a possible cause of an adverse event that can cause harm to the training processes, to a student, employee or institution as a whole. Damage or negative effects occur as a result of the realization of the threat.

2.2 Vulnerability

Vulnerability is defined as a weakness in a process, in humans, or in resources (assets) that one or more threats can "exploit" and thus cause an incident or damage (loss) to the process, people or the institution as a whole. It is a weakness on the elements of the internal context that is least "resistant" to threats. This weakness is the most visible source of risk in the process or institution. It is important to emphasize that vulnerability is always monitored with threats from the environment or within the system itself. Threats without vulnerability have no effect on risk, that is, if there is no vulnerability in the process (institution), the magnitude of the threat is irrelevant. The reverse is also true. So, if there are no threats in the process (institution), the intensity of its vulnerability is irrelevant. Vulnerability reduction must be a constant concern of all stakeholders in the systems, and especially of employees who perform the highest functions, as it is the most efficient and best way to reduce risk.

2.3 Consequence

The consequence is most often defined as the result of the interaction of threat and vulnerability, that is, the condition when the threat exploited the vulnerability and thus led to the occurrence of damage in the higher education institution (processes, projects, etc.).

This consequence or harm is most often expressed in financial indicators.

The consequences can be both negative and positive.

2.4 Risk Criteria

Risk criteria are reference points that can be determined by internal rules, agreements, norms, rules of practice, contracts or other documents, and represent a measure or an expected goal. Criteria are used to assess the level and significance of the risk to be considered or assumed.

For example, a reference point or criterion may be: minimum value, maximum value, "from – to" reference area, indices, time, financial indicators, etc.

2.5 Risk Owner

Risk Owner is defined as a natural person or legal entity that has assumed the responsibility of risk management and is responsible for and assumes all the consequences of the risk.

3 RISK CLASSIFICATION

There is no universally applicable uniform classification by which risks can be categorized. The approach to risk classification depends largely on the specific nature of each organization's business activity. At the same time, generic risk classification into strategic and operational risk categories is useful. Such a division makes it possible to systematically look at a potentially unlimited number of risks and to more easily determine which level of management will primarily address which risk category.

3.1 Strategic and Operational Risks

Strategic risks are risks associated with the achievement of the medium- and long-term goals and strategic priorities of a higher education institution. These are the risks the consequences of which are addressed to wider interest groups and end users of services (students), stakeholders, etc. Strategic risk management should be an integral part of the key decision-making process at the highest management level within the strategic/mid-term planning, monitoring and evaluation of the implementation process of adopted plans.

Examples of strategic risks at higher education institutions include:

- a) Risks related to failures in the implementation of public policies under the jurisdiction of the institution.
- b) Risks involving the activities of not initiating development processes and following current trends in the field of education.

- c) Risks related to the institution's ability to ensure long-term financial sustainability.
- d) Risks related to changes in the demographic and socio-economic trends of service users and the institution's ability to respond to them.
- e) Risks related to fraud, corruption or abuse that undermine citizens' confidence in the institution of public action.
- f) Risks associated with technological changes and the institution's ability to respond to and use them in training processes.
- g) Risks related to current or potential changes to national or European law in the field of education.
- h) Risks related to environmental change, climate change (floods/droughts) and their impacts on the environment and quality of life and functioning of institutions.
- i) Service competitiveness and the institution's ability to deliver value to service users.
- j) Risks related to failure to meet current and future needs/expectations of service users (students).

Operational risks are risks associated with the implementation of activities and processes within individual processes in an institution. These are risks that generally relate to the business activity of a higher education institution, within the prescribed deadlines, in accordance with the indicators of the realization of goals, and in accordance with the required quality and applicable laws and procedures. Operational risk management is part of the day-to-day operations and is the responsibility of the executives responsible for the programs, activities and processes, or managers of the organizational components within which these programs, activities and processes are implemented.

- a) Risks related to the professionalism and ethics of the employees in performing training activities.
- b) Risks related to financial misconduct.
- c) Risks related to violation of regulations, lawsuits, external judgments (self-analysis, re-accreditation, etc.).
- d) Risks related to the safety and health of employees and students.
- e) Infrastructure risks and risks related to technical aids in processes.
- f) Risks related to suppliers and delivery of various goods and materials.
- g) Operational risks related to the security of IT systems, equipment, data, etc.

Although the division of risk into strategic and operational is useful, it should be kept in mind that these two risk categories cannot be viewed in isolation from each other. The interrelation of strategic and operational risks stems from the fact that operational risks can be the cause or effect of strategic risks and vice versa. Causal links and correlations between strategic and operational risks need to be addressed at all stages of risk management.

3.2 Inherent and Residual Risks

On the technical side, two types of risk can be distinguished: inherent and residual risk (Fig. 2).

Inherent risk is the risk or set of risks that an institution faces without considering the established controls in place. This is a type of risk where there are no controls and activities that mitigate the risks. They are caused by the usual circumstances and types of activities being carried out, which may be internal and external.

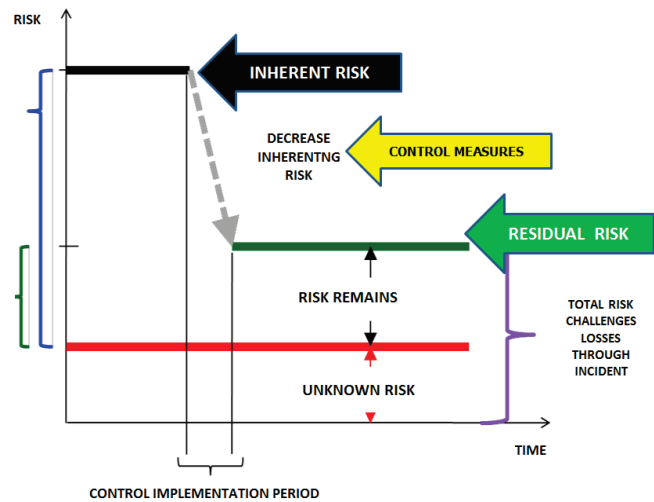


Figure 2 Inherent and residual risk [3]

Residual risk is the risk or set of risks that remains after processing (treating) the risk. If this risk is to be accepted then it must be approved by the highest management of the institution. The risk remaining after applying new or expanded controls is residual risk. Neither system is immune to the risks, nor they can be completely eliminated with all controls applied. If the residual risk has not been reduced to an acceptable level, the risk management cycle must be repeated to identify a way to reduce the residual risk to an acceptable level.

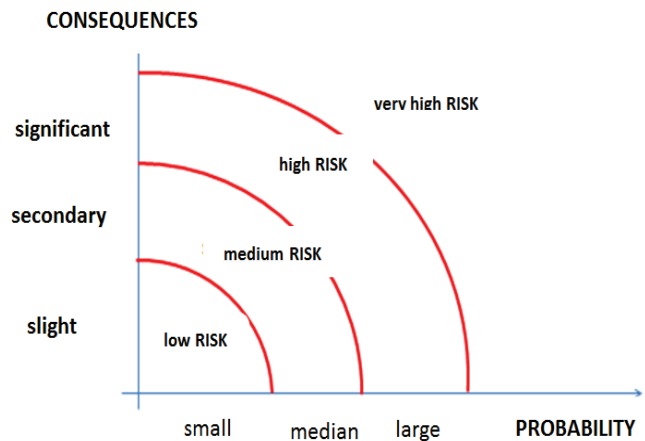


Figure 3 Risks by intensity

3.3 Division of Risk by Intensity

According to the impact intensity, the risks in higher education institutions can be divided into (Fig. 3):

- 1) small risks (negligible),
- 2) medium risks (small),
- 3) high risks (high) i
- 4) very high risks (extreme).

3.4 Division of Risk by Relatedness

Risks in higher education institutions can be grouped according to relatedness, such as:

- risks that may be affected;
- risks that cannot be affected;
- risk of failure to comply with legal frameworks;
- the risk of incorrect recording;
- the risk of incorrect reporting;
- visible risks;
- hidden risks;
- external stakeholder risks;
- risks with archiving information;
- external risks;
- internal risks;
- specific;
- information security risks;
- personnel risks, etc.

4 RISK MANAGEMENT

Risk management at higher education institutions can be defined as a set of designed and planned activities that are systematically undertaken to minimize the negative impact of risk on training processes and learning outcomes. In other words, it is necessary to find an acceptable combination of cause and effect tolerance that enables actions to reduce adverse events that call into question the normal functioning of the training process.

Risk management is also required by international standards for management systems (quality, environment, security, energy, etc.). In this regard, higher education institutions are required to identify and analyse them in order to take steps to:

- ensure that the quality assurance system can achieve the intended results;
- improve the desired effects;
- prevent or minimize unintended consequences, and
- achieve planned improvements.

For example, the standard [6] requires of the institutions to assess risk when designing a quality assurance system, taking in account the external and internal context and the needs and expectations of all stakeholders in the training process. For a more specific application of the requirements of this standard, a more detailed application of the referenced literature is recommended [3, 7, 8].

Managing risks means knowing the conditions and factors that lead to the consequence of which the institutions' leaderships must have some knowledge and various

information and data at their disposal. Therefore, for effective risk management, it is necessary to effectively manage the information on which different decisions are made. The interdependence of quality assurance, risk management and information management is shown in Fig. 4. It is important to note that a basic prerequisite for effective and comprehensive quality assurance management is the need for a sound risk and information management system [9].

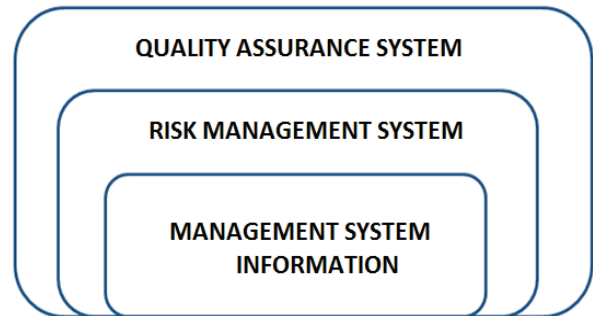


Figure 4 Management system interdependency

Risk management at higher education institutions cannot be considered separately from the strategy and operational education procedures. For the purposes of risk management, an operational procedure should also be defined.

The purpose of the procedure is to describe how the institution intends to implement a systematic approach to risk management and to develop a methodology for risk management processes tailored to the specificities of the particular institution. Risk management is part of the business education system and it is not advisable to look at it separately. It must be an integral part of all operational activities, major projects and defining significant goals in the education and business process. The goal is to recognize the factors and take preventive measures so that the risk does not adversely affect the realization of the defined activities and goals.

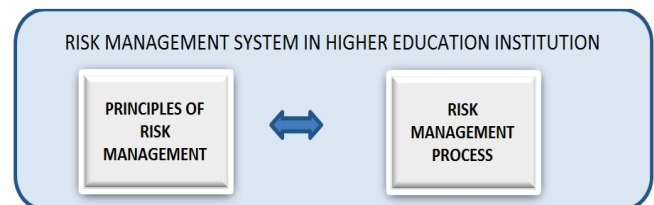


Figure 5 Risk management system

For a successful risk management system in higher education institutions (Fig. 5), it is important to understand and apply the general principles and have an effective risk management process [4]. Its purpose is to increase the likelihood that an institution will realize its goals through the management of threats and adverse situations, and be prepared to seize the opportunities that may arise.

4.1 Risk Management Principles

The most important principle of risk management in higher education institutions is to prevent events that could cause risk in processes, projects and other activities and thus cause harm. In addition to the above, other principles must be applied, such as:

- Risk management should be an integral part of the process map in higher education institutions with defined process features and in synergy with the main, ancillary and management processes [10].
- They must be an integral part of the decision-making system at all levels of management, and raise awareness with stakeholders about their importance in the training and business processes.
- Risk management is the systematic, structured and timely activities of all the leaders and processes in the institution.
- Risk management always adapts to specific situations.
- Risk management is dynamic, repeatable and sensitive to change.
- Risk management explicitly addresses all types of uncertainty in training processes.
- Risk management facilitates the continuous improvement and improvement of the quality of education, processes and the institution as a whole.

It is important to emphasize that all stakeholders should uphold the principles outlined above, as well as the principles of good practice that they receive during the functioning of the education process.

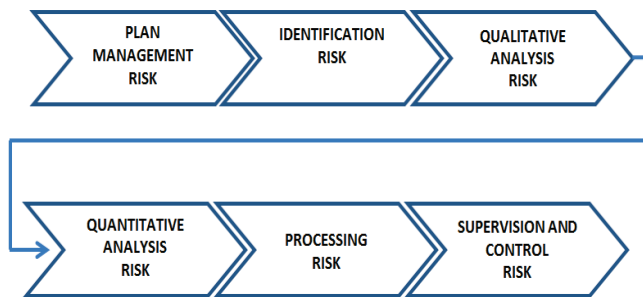


Figure 6 Risk management process

4.2 Risk Management Process

The process of risk management in higher education institutions [11, 12] can be observed through the following activities (Fig. 6):

- 1) Risk management planning - the process of defining how risk management activities will be carried out for a process, project, etc.
- 2) Risk identification - The process of identifying those risks that may affect an event or project and documenting their features.
- 3) Qualitative risk analysis - the process of prioritizing risk for further analysis or action by assessing and combining the probabilities of their occurrence and impact.

- 4) Quantitative risk analysis - the process of numerically analysing the effect of identified risks on the overall objectives of a project or event.
- 5) Risk Response Planning (treatment) - the process of developing options and actions to improve opportunities and reduce the dangers that threaten the goals of an event or e.g. a project.
- 6) Risk monitoring and control - the process of implementing risk response plans, monitoring identified risks, monitoring residual risks, identifying new risks and evaluating the effectiveness of the risk process during, e.g. a project.

4.2.1 Risk Management Planning

It is defined as documented information that describes the ways in which an organization will manage risks.

The risk management plan specifies:

- tools and methods,
- approaches (scope),
- responsibilities, roles,
- resources (amount of funds) that will be used to manage the risks.

4.2.2 Risk Identification

It is a process that identifies which risks can affect the results, project, goals and documentation of their features. Basically, the answer is: how and what can happen badly or well and when?

The following sources of information and data can be useful for risk identification [13, 14]:

- Empirical research (regional, national, international, local, etc.);
- Opinions of experts and scientists (experts in specific issues);
- Results of different analyses of study success;
- Results of self-analyses carried out; internal and external judgments in the quality assurance system;
- Results of accreditation of higher education institutions;
- Various interviews and surveys of all stakeholders in the education process;
- Discussion with focus groups;
- Strategic business management (SWOT, BSC, etc.);
- Reports of insurance companies;
- Results of reviewing the effectiveness of the quality management system by the highest management of the institution, etc.;
- Miscellaneous financial statements;
- Various professional publications;
- Reports from the analyses carried out in management systems (non-conformities, complaints, corrective actions, etc.);
- and other information.

During the risk identification it is possible to notice:

- 1) Known risks (Risks identified very quickly, usually after initial analysis).

- 2) Predictable risks (Risks that may be encountered - identified based on past experience).
- 3) Unpredictable risks (Risks that can occur but are very difficult to identify in advance).

4.2.3 Qualitative and Quantitative Risk Analysis

Qualitative risk analysis is the process of prioritising risks for further analysis or action by assessing and combining their likelihood of occurrence and impact.

Quantitative risk analysis is the process of numerically analysing the effects of identified risks on overall project objectives or defined operational objectives. It is conducted over risks that are prioritised in the process of qualitative risk analysis (risks that significantly affect the goals).

Known FMEA analysis [6] and probability theory are most commonly used to perform these analyses [7]. Probability is defined as the possibility of an event occurring in a defined period of time. Each event consists of outcomes. If there are n outcomes then there are 2^n events.

Events as occurrences can be [15]:

- Safe ($p = 1.0$)
- Impossible ($p = 0,0$)
- Random (p from 0.0 to 1.0).

If the probability of an event is denoted by (p) and if $p = 1$ then that event is said to be safe. If the probability of an event is equal to $p = 0$, that event is impossible. A random event is an event that may or may not occur when certain conditions are met. An event that rarely happens is less likely, if it happens more often, is more likely. If it occurs in all cases, it is most likely, so it is said to be an almost certain event [16].

4.2.4 Risk Treatment

In fact, a process aims to reduce the level of risk through multiple steps using different tools. Treatment must be thorough but cost-effective [13]. Once a risk has been identified, analysed and evaluated, it can be accessed in one of the following ways:

- try to avoid it or not,
- if it cannot be avoided there is a possibility of risk transfer
- if it cannot be avoided there is a possibility of risk reduction
- if it cannot be avoided there is a possibility of risk acceptance
- we consciously take it to take the opportunity.

4.2.5 Risk Control

The risk control process is:

- implementing risk response plans,
- monitoring of identified risks,
- control of residual risks,
- identifying new risks and
- assessing the effectiveness of risk-related processes.

5 PRACTICAL APPLICATION

The full functioning of quality assurance systems at higher education institutions is not possible without defining and implementing a process that manages risks and opportunities. This process must be recognised with all its elements of input, processing and output as well as indicators of its success [17].

Table 1 Identification, analysis and assessment of risk

RISK EVALUATION										
INSTITUTION:										
Process / Project:				Strategic risk:		Operational risk:		Project risk:		
Created:			Date:		Reviewed:		Remark:			
Ordinal number:	Risk description (consequence event)	It is assumed that there is no control (control mechanisms) INHERENT RISK LEVEL			Control mechanisms (Current risk control)	Responsible person	Residual risk assessment - when control mechanisms are in place RESIDUAL RISK LEVEL			Date of revision
		Influence (1-5)	Probability (1-5)	Risk rating NR (1-4) UR (3-8) VR (5-15) ER (10-25)			Influence (1-5)	Probability (1-5)	Risk rating NR (1-4) UR (3-8) VR (5-15) ER (10-25)	

5.1 Stages in the Process of Applying a Risk Management System

The operational risk management system in higher education institutions can be practically implemented through the following steps:

- 1) Identification of risk issues and their importance;

- 2) Orientation on a perceived problem;
- 3) Decision making by the highest management of the institution;
- 4) Appointment of a risk coordinator;
- 5) Adopting a risk procedure or rulebook;
- 6) Development of a risk management plan;
- 7) Identification of risk in processes;
- 8) Analysis of identified risks;
- 9) Assessment of inherent and residual risks;

- 10) Defining treatments for assessed risks,
- 11) Supervision and control of risk measures.

A similar situation is with regard to risk management during the implementation of different projects at the institution and when defining strategic goals.

Tab. 1 can serve in the procedures of risk identification, analysis and assessment, while Tab. 2 can be successfully used in defining treatment activities for high-intensity risks.

Table 2 Risk treatment

Ordinal number:	Risk code	Risk description	Risk Rating NR (1-4) UR (3-8) VR (5-15) ER (10-25)	Risk treatment A - Avoidance T - Transfer R - Reduction Ac - Acceptance	Description of activities that are planned to be taken at residual risk	Responsible person
1.						
n.						

5.2 Methods and tools in Risk Management Processes

Different techniques (tools and methods) need to be known and used in practical risk management procedures. None can capture all the risks that are identified in education processes. Some are only suitable for identification or analysis. Others are for evaluating or defining treatments, and there are some that are appropriate for more than one activity.

Some of the qualitative techniques that are recommended in risk assessment are:

- What-If Analysis
- Flowchart/Process mapping
- Brainstorming (PESTLE, SWOT, etc.)
- Hazard and Operability Study, HAZOP
- Failure Mode and Effect Analysis, FMEA
- Failure Mode, Effect and Criticality Analysis, FMECA
- Risk Matrix
- Risk Register
- Safety Review
- Relative ranking, etc.

Some of the quantitative techniques that are recommended in risk assessment are:

- Fault Tree Analysis, FTA
- Event Tree Analysis, ETA
- Probabilistic Safety Assessment, PSA
- Probabilistic Risk Assessment, PRA
- Risk Matrix
- Risk Register
- Rapid Risk Assessment, RRA
- Reliability Analysis
- Human Reliability Analysis, HRA
- Markov Chain Analysis, etc.

5.3 Risk Register

At least one risk register shall be established at the institution level, which shall include information on strategic and operational risks. The risk register shall be updated as necessary and at least annually as part of the regular review by the top management of the quality assurance system to monitor the implementation of the planned risk mitigation measures. When updating the register, information about emerging risks is also entered.

In principle, the risk register shall contain at least the following information:

- Risk Identification Code
- Risk category (strategic or operational)
- Brief description of risk (cause and effect)
- The level of total risk exposure
- Area of risk impact
- Risk management measures (treatment)
- Persons responsible for implementation of measures and deadline for implementation.

5.4 Risk Coordinator

The person in charge of the institution is responsible for establishing a risk management system. The heads of its organisational components are responsible for managing the risks that may affect the achievement of the objectives within their competence, that is, related to the functions, activities and processes within their competence.

Practice shows that it is advisable to appoint a strategic risk coordinator and an operational risk coordinator.

The tasks of the strategic risk coordinator are:

- a) collecting information on strategic risks;

- b) organizing discussions on the data collected and prioritising the identified strategic risks;
- c) recording strategic risks in the risk register and monitoring the management of those risks;
- d) updating the information in the risk register based on the collected risk status data.

The tasks of the operational risk coordinator are:

- a) collecting information on operational risks related to processes;
- b) organizing discussions with the organisation component managers on the data collected and the results of the risk assessments where priority operational risks are identified;
- c) entry of operational risks in the risk register and monitoring of operational risk management;
- d) updating the information in the risk register based on the collected risk status data.

5.5 Performance Indicators for Risk Management Processes

For monitoring the efficiency and effectiveness of the risk management process, some of its essential key indicators are the following:

- Risk management should be a regular point in meetings of bodies, departments, councils and other bodies to allow risk exposure to be considered and the priorities set.
- The risk register should be updated regularly after the new situation.
- Each identified risk must have its own status in terms of intensity and treatments undertaken.
- Each risk must have a responsible person for its monitoring, control, reporting, etc.

6 CONCLUSION

Higher education institutions can have multiple benefits by implementing risk management systems and processes, such as:

- increasing the likelihood of achieving the defined goals,
- encouraging the highest leadership of the institution to be proactive,
- making quality decisions based on the analysis and risk and opportunity assessment,
- the possibility of preventive acting on the problems that have not yet occurred,
- reviewing the experiences of other similar institutions and initiating adequate activities,
- raising the awareness of all stakeholders to identify and adequately treat risks,
- more efficient use of all available resources,
- increasing the readiness and reliability of all processes and projects implemented in the institution,
- increasing compliance with legal and other relevant regulations,
- recognition of other relevant risks,

- improving the functioning of the process while improving resilience to problems, etc.
- elimination or reduction of losses that may occur in training processes,
- improving the health and safety of students and employees and protecting the environment,
- etc.

7 REFERENCES

- [1] ISO/IEC Guide 5:1999. Risk management – Vocabulary.
- [2] Dolečak-Alduk, Z., Sigmund, V., & Lončar-Vicković, S. (2008). Osiguranje kvalitete visokog obrazovanja u europskom obrazovnom prostoru. *Tehnički vjesnik*, 15(1), 39-44. (In Croatian)
- [3] ISO IEC 31010:2018 – Upravljanje rizicima – tehnike za procjenu rizika (Risk management — Risk assessment techniques).
- [4] Adelsberger, Z. (2010). ISO 31000 i generički pristup upravljanju rizicima. *Zbornik radova 10. Hrvatske konferencije o kvaliteti*, HDK, Šibenik. (In Croatian)
- [5] Kondić, Z., Maglić, L., Pavletić, D., & Samardžić, I. (2019). *Kvaliteta 1, 2, 3*. Sveučilište J. J. Strossmayera u Osijeku, Sveučilište Sjever, Sveučilište u Rijeci, Varaždin. (In Croatian)
- [6] McDermott, R. E., Mikulak, R. J., & Beauregard, M. R. (1996). *The basics of FMEA*. Productivity Inc., New York.
- [7] ISO/TR 31004:2013; Upravljanje rizicima - smjernice za provedbu ISO 31000 (Risk management - Guidance for the implementation of ISO 31000).
- [8] ISO 9001:2015; Sustav upravljanja kvalitetom – Zahtjevi (Quality management systems – Requirements).
- [9] Boban, M. (2017). Upravljanje kvalitetom u visokom obrazovanju i analiza rizika. *18th International Symposium on Quality – Kvaliteta kao strategija / Quality as strategy* Vodice, 279-289. (In Croatian)
- [10] Srića, V. (2011). *Mendžment rizika*. Velučilište u Šibeniku, Šibeni., (In Croatian)
- [11] Ivković, M. (2009). *Osiguranje kvalitete u visokom obrazovanju*. Geodetski fakultet Sveučilišta u Zagrebu, Zagreb, p. 21. (In Croatian)
- [12] Sprčić, M. (2013). *Upravljanje rizicima*. Sinergija, Zagreb. (In Croatian)
- [13] Jakovičević, D. (2016). *Osiguranje i rizici*. Sveučilište u Zagrebu, Ekonomski fakultet, Zagreb. (In Croatian)
- [14] Andrijančić, I., Gregurek, M., & Merkaš, Z. (2016). *Upravljanje poslovnim rizicima*. Plejada – Libertas, Zagreb. (In Croatian)
- [15] Buhlmann, H. (1970). *Mathematical Methods in Risk Theory*, Springer-Verlag, BHNy.
- [16] Lam, R. (2003). *Enterprise Risk Management From Incentives to Controls*, Hoboken, new Jersey, John Wiley & Sons.
- [17] Lučin, P. (2007). *Osiguranje kvalitete u Europskom visokoobrazovnom prostoru, Kvaliteta u visokom obrazovanju*. Nacionalna zaklada za znanost, visoko školstvo i tehnološki razvoj RH, Zagreb, p. 21. (In Croatian)

Authors' contacts:

Živko Kondić, PhD, Prof.
University North,
Trg dr. Žarka Dolinara 1, 48000 Koprivnica, Croatia
E-mail: zkondic@unin.hr

Željko Knok, mr. sc., senior lecturer
Polytechnic of Međimurje in Čakovec,
Bana Josipa Jelačića 22a, 40000 Čakovec, Croatia
E-mail: zknok@mev.hr

Veljko Kondić, mag. ing. mech.
University North,
Trg dr. Žarka Dolinara 1, 48000 Koprivnica, Croatia
E-mail: veljko.kondic@unin.hr

Sanja Brekalo, PhD
Polytechnic of Međimurje in Čakovec,
Bana Josipa Jelačića 22a, 40000 Čakovec, Croatia
E-mail: sbrekalo@mev.hr