ISO 31000 – Prerequisite for Strategic Risk Management in the Activities of Organizations

Assoc. Prof. Dr. Radka Ivanova
University of Economics - Varna, Bulgaria
r.ivanova@ue-varna.bg

Abstract

Each sphere of human activity is accompanied by risk-related situations, regardless of the size, the subject matter, the scope, and the geographical location of the organization. The many internal and external factors and influences, to which the entities are subject, create conditions of uncertainty as to the timing and extent of their objectives. Some of the risks can be predicted and others may not, which requires the systematization of specific actions to help organizations adapt to change more easily and quickly. Achieving this requires clarifying the specifics of risk situations and finding the right approach to them. The purpose of this article is to characterize the specificities of the risk and to analyze the importance of ISO 31000 in defining the responsibilities of organizations for its management.

Keywords: Risk, Risk Management, ISO 31000:2018

JEL Code: O10; O20; M210

Introduction

The turbulence of the environment confronts organizations with a host of unknown factors, with the impact of which they have to deal with. In the course of carrying out their activities, different risks occur in one way or another, which hinder the achievement of the objectives set. This requires assessing the likelihood of risk situations occurring and the impact they will have on organizations, defining specific measures, monitoring, and controls to form behavior adequate to the newly created situation. This requires the development of a system allowing risk management and its adaptation to the specificities of the specific organization. In this regard, the International Organization for Standardization develops ISO 31000: Risk Management, which focuses on comprehensive problem solving through appropriate planning and management practices.

1. ISO 31000: Risk Management

1.1. Risk and Risk Management

The conditions in which organizations must operate today are constantly changing, characterized by varying degrees of risk. The reason for this lies in the fact that it is difficult to predict any changes in the factors characterizing the external and internal environment. The term 'risk' is used in all areas of people's activities, although it is considered to appear in Europe after the 14th century, and its wider application is linked to the statistical examination of risk calculations in insurance and gambling (Krastev, 2020, p. 122). The concept of risk, as a means of reducing the degree of uncertainty in determining insurance premiums, is gradually finding much wider importance. A prerequisite for this is the fact that at the end of the 20th century and the beginning of the 21st century. Mankind witnessed a progressive increase in hazards defined as risks (Lalonde & Boiral, 2012:278). In general, the risk is associated with any danger and/or threat having a negative impact on people and organizations. The risk is seen as a deviation from the results that occur in a particular situation (Eykova, 2013:16). This deviation is negative and affects the interests of individual organizations, their staff, and the actions taken by them. The specialized literature also states that from a systematic point of view we can characterize risk as to the possibility of frequent or continuous changes in the organization's security environment (Georgiev, 2007).

In ISO 9000:2015, item 3.7.9, the term risk is defined as the uncertainty effect. The traceability

of the etymological origin of the term "risk", as the researchers in the field point out, shows that it is of a contradictory nature (Krastev, 2020 et al.). From Arabic, the word "risq" comes down to opportunities for profit and is favorable. In Latin, the word "risicum" means barriers that need to be overcome, while in English "risk" comes down to some loss and has a negative character. In general, we can point out, that the risk represents an estimated degree of uncertainty as regards the achievement of the expected results in the course of the implementation of the strategy (Zafirova, 2017:210). In this respect, in practice, the risk is based on the degree of uncertainty of the internal and external environment of the organizations. Its sources may be of an objective and/or subjective nature, with the result that different persons, groups, and organizations, independent or related events, phenomena, and natural and societal processes should be considered as sources of risk. In general, the specialized literature comments on the thesis that risk is associated with phenomena that manifest themselves against the will of the people and, accordingly, situations in which the role of the man is leading (Krastev, 2020). In order to assess the risk, it is necessary to describe and analyze all possible possibilities for something unwanted to happen, including fatal. At the same time, we should point out that, according to some researchers, the risk represents a measurable magnitude; multidimensional characteristic of future conditions; connection with random events and processes; occurs as a result of interactions between nature, humans, and technology; possibility of a positive outcome in the event of the uncertainty of the actions carried out (Ivanova, 2020:96). The risk shall also be identified by the likelihood of loss and injury occurring and realizing, a deviation from the expected negative results, as well as actions of an inappropriate nature requiring higher determination and rapid response. On the one hand, globalization creating new risks and consequences is a prerequisite for its emergence and, on the other hand, natural disasters generally cannot be managed by people and organizations and they are obliged to comply with them. In addition, the risk can also be defined as the effect of uncertainty to achieve organizational objectives. In general, risk is defined as uncertain events that may affect the general condition of an individual or organization (Gerunov, 2020:24).

The risk description is directly dependent on its type, which is why we will indicate that there are different varieties of risks. In general, risks are distinguished by technological, market, financial, economic, public, environmental, political, reputational risk; risks related to cooperation between partners, intellectual property, customers, staff, knowledge, and management. From the point of view of risk management standards, classification is based on external and internal factors, impact on organizations, and more precisely, strategic, operational, financial, and physical hazard risk (Krastev, 2020).

With regard to deviations of the actual results from the expected ones, specialists bring out two types of risk – "clean" and speculative (Georgiev, 2007; Gerunov, 2019; Krastev, 2020; Kuznetsova, 2004:26). Pure risks (hazards) are bound by the possibility of zero or negative results and are rather defined as natural and natural. From this point of view, organizations must provide for such actions to allow them to minimize negative consequences since they cannot influence their manifestation. The manifestation of speculative risks, in turn, leads to losses, and when they are not manifested, the organizations will realize benefits (profits).

Some researchers highlight the fact that determining risk as a process covers identifying the causes and sources of risk, events, situations, or circumstances that may potentially have a material impact on the objectives and nature of that impact (Stoev, 2017:226).

At the same time, it is considered that the risk in modern business performs four main functions: innovative; regulatory; protective; Analytical (Fomichev, 2020). They can be considered separately, but they also have several intersections between them.

The specificities of risk clearly demonstrate the need for targeted management in this area. In essence, risk management must be strategic in order to deliver real benefits for organizations. Defining specific long-term actions to address the risk situations in which subjects find themselves

in changing expected factors is a prerequisite for successful crisis management. Risk management should therefore be integrated into the strategic management and organizational culture of companies in order to transform strategic solutions into tactical and operational tasks that staff know and perform accordingly. Like any other management and risk management, it is a cyclical process that involves continuous identification and analysis of changes in the expected state of the external and internal environmental factors. The success of risk management is closely linked to assessing the past, present, and future; as well as all actions and objectives of the organization. According to some authors, risk management should therefore be seen as a system of activities that are linked to identifying and analyzing risks, developing alternatives, and making decisions to maximize positive effects and minimize negative ones in different risk situations (Krastev, 2020, p. 132). When choosing specific decisions on the behavior of organizations in exceptional circumstances, the risk appetite of the decision-makers is relevant. The preference only for lower-risk solutions as well as predominantly high-risk solutions can have an equally negative impact on the organization. Therefore, more balanced options should be sought and leaders making the final choice should overcome their own preferences.

Risk management as a process is defined by some researchers as a logical structure that encompasses defining objectives and defining the criteria for achieving them, identifying risk areas and specific risks, assessing risks, and taking concrete measures to address possible threats to achieve the objectives (Lecheva, 2020:191). Establishing the right approach to risk management can be seen as a successful prerequisite for preventing several negative consequences for organizations. For an organization to use risk management as a source of competitive advantages, it should be able to manage operational risk to achieve its long-term strategic objectives (Yordanova, 2020:79). Risk management should also be seen as an iterative process covering all stages of the organization's life cycle, starting with identifying possible risks, analyzing risks, planning their management, follow-up monitoring, and periodic follow-up analysis. The latter ensures proper identification of the level of effectiveness of the risk management process in the organization.

Risk management can also be defined as a process related to identifying, planning, controlling, minimizing, and even eliminating hazards, if possible. The successful implementation of this process involves developing a special plan to analyze the risks and costs associated with them, make specific decisions, practical implementation, testing, and safety assessment. An important point is the timely identification of the threats to which all the assets of the organizations are exposed – tangible, financial, technological, information, human resources, etc., to provide for adequate measures for their protection. In this regard, it is of great importance to analyze the potential hazards and uncertainties that companies may face in the course of achieving their objectives and to provide for preventive safeguards to minimize the adverse effects of risk situations. Some researchers come from Henry Mintzberg's philosophy of 5 Ps for Strategy (Plan, Ploy, Pattern, Position, Perspective) and bring out four main risk management strategies, namely:

- avoiding (ignoring) risk;
- damage prevention;
- risk acceptance;
- transfer (sharing) of risk.

Each of them has its own peculiarities and would be suitable for application under different conditions, including according to the capabilities of the particular organization. Risk avoidance is associated with taking action that will allow it to be mitigated. The prevention of damage involves the use of own resources to cover such in the event of possible risk situations. The acceptance of the risk comes down to awareness of the adverse situation and its acceptance, as it cannot be prevented. The transfer of risk is linked to its transfer to another organization, which is most often carried out through insurance, outsourcing and hedging can also be used.

On the other hand, the approaches used to analyze risks are considered to be divided into two main varieties, fragmented and comprehensive risk assessment, depending on whether some or all of the alternatives are considered and, respectively, what countermeasures are sought. Each organization chooses the approach to apply itself, and at different times of its development, it can change the approach used.

We should also point out that there is an understanding in the literature that risk management is associated with going through several basic steps, which are limited to setting targets; identification and assessment of risks; selection of risk reactions; documenting the risk management process and, of course, monitoring to assess the achievement and extent of dealing with risk situations (Lecheva, 2020:186). As an essential element of risk management, practice shows that its assessment can be derived as it helps managers to become more aware of the specificities of the risks they face. In this respect, the risk assessment shall be presented as a process consisting of risk identification, analysis, and assessment.

As regards how it is carried out, the risk management itself should be carried out at several levels, namely: strategic, process, and personal, to cover the overall management of the organization, the main business processes taking place therein, as well as the risks associated with the work of the individual participants in those processes. The attention of the senior management of each company should be focused on the risk management system, supporting different aspects, and making relevant strategic decisions. In support of the managing authorities and given the importance of risk management, the International Organization for Standardization (ISO) shall develop a special standard under the number ISO 31000. The procedures and actions, set out therein, aim to prepare organizations implementing the standard for easier handling of risk situations.

1.2. Features of ISO 31000:2018

The ISO 31000 Risk Management standard is designed to define the basic principles and guidelines for risk management faced by organizations at different times in their development. The standard allows it to be used in both the public and private sectors, regardless of the nature of the risk and its consequences (positive or negative); to provide common methodology and rules for risk management. Risk management is defined in ISO Guide 73 as a set of coordinated activities to guide and control organizations in terms of risk (Proenca, Borbinha, Vieira, 2017). The standard uses two concepts: Management Risk and Managing Risk, and the distinction between them is limited to the following: Management Risk involves clarifying the principles, framework, and management process while Managing Risk is associated with the application of these principles in the activities of organizations. An important feature is the fact that the scope of risk management may be different – to apply to the whole entity, to its individual divisions, functions, projects, or activities. Risk management should be seen as a process related to the systematic implementation of a set of practices, policies, and procedures for the successful management of context-based activities and risk identification, its analysis, overcoming, and monitoring. The communication strategy chosen by the management of the organization is important, as it should ensure timely transmission of information in order to form a credible picture of the situation in which it is located on the different time horizons. Of particular importance for risk management success is the identification of internal and external factors negatively influencing development and activity in order to establish the correct context in which risk should be considered.

The implementation of ISO 31000:2018 provides several advantages for organizations, including the following:

- better awareness of the possible risks and their consequences by the employees;
- achieving greater responsibility among all those working in the organization, regardless of the position they hold;

- more effective and efficient management of business processes;
- improving the image of the company, its products, and services, etc.

This in practice means creating the conditions for maintaining the sustainable competitiveness of organizations. In creating successful risk management practices, prerequisites are created to transform the uncertainty in which companies must operate into strategic opportunities.

As a result of the risk assessment, actions aimed at mitigating the negative impact of the identified risks are identified. ISO 31000 implies that risk management is an integral component of overall governance in organizations in order to allow successful adaptation to change, taking into account the specificities of the processes in the specific entity. As per the standard, each organization needs to determine the entire risk in terms of its nature, which events or circumstances may provoke it, what are the possible consequences that can be expected. ISO 31000 implies a description of the possible risks, their hierarchical arrangement depending on their degree of significance and impact. It achieves transparency of risk management as an integral part of the processes taking place in an organization, taking into account relevant human and cultural factors. Also, ISO 31000 requires the consideration of risk management as a dynamic and repetitive process in order to create prerequisites for an adequate response to oncoming external and internal changes.

Effective implementation of the standard requires a preliminary precise assessment of the organization in terms of its internal and external components in order to determine with maximum accuracy its condition and specificities (Risk management, 2009:10). It is considered that the external assessment of the organization should focus on three main strands, namely:

- the components of the external environment (macro and microenvironment) in which the entity concerned must carry out its activities – political, legal, economic, social, technological, financial, cultural, natural factors, competitors, consumers, etc., being considered locally, regionally, nationally, internationally depending on the specific needs;
- the leading development trends that prejudge the objectives of the organizations;
- the specificities of stakeholders and their relationships.

The analysis of the internal environment of the entities covers the whole organization and all its structural components, which implies an assessment of:

- the organizational structure in terms of its effectiveness, given the management method adopted; characteristics of the roles and status of staff;
- the objectives, policies, strategies adopted;
- the resources available and the need for them;
- the information systems used, the direction of information flows and the decision-making styles applied;
- organizational culture, values, standards of conduct;
- relationships with internal stakeholders;
- the specificities of the contractual relationship, etc.

Successful risk management requires it to be part of all practices and processes taking place within the organization, including at the level of their development. A risk management plan is also needed to ensure that this governance is carried out in practice and is a component of the overall strategic plan of the organization. Given the global transformations and new situations faced by all countries today, risk management should be seen as a means of achieving competitive advantages. Overall, the responsibility for dealing with risks rests with the management of the organization, which is why it must find a way to analyze and address them more effectively. At the same time, it should not be forgotten that decisions of senior managers are implemented by the remaining staff in the organization, and therefore the risk management strategy, and objectives must be shared by all. On the other hand, ISO 31000 entails the supervision and control of activities carried out within its scope, which are supported by the documentary equipment inherent in that standard. Risk information is part

of the management information of the organization as a whole and is therefore used by its management for follow-up analyses and specific actions.

ISO 31000 was first published in 2009 and its objective is to integrate risk management into the overall governance of organizations, strategically and operationally. Subsequent revisions to the standard lead to appropriate adjustments, as a result of which its new version is published in 2018, up to date today.

The guiding principles of risk management according to ISO 31000 set out in Standard Deviations (2018:9) are limited to the following eight:

- Personality and proportionality of the framework and processes.
- Appropriate and timely stakeholder involvement.
- Structuring and comprehensiveness.
- Risk management is an integral part of all organizational activities
- Anticipating, detecting, recognizing, and responding to changes.
- Taking into account the limitation of the information available at a given time.
- Human and cultural factors influence risk management.
- Continuous improvement of risk management through training and experience.

The first five principles define how risk management should be designed in the organization, and the last three – show how this governance should work. In practice, the first five principles come down to proportionality, equality, inclusiveness, built-in, and dynamics. The manifestation of these principles can be described as follows: risk management actions must be commensurate with the risk to the organization; be equivalent to other activities therein; the risk management approach is characterized by integrity; risk management actions to be dynamic and consistent with and change in risks. Risk management mechanisms need to be implemented in such a way as to allow continuous improvement.

Overall, ISO 31000 focuses on leadership and engagement of managers and everyone else in the organization in terms of flexible risk management by developing an adequate policy and strategy in this area. Comparing ISO 31000:2018 with ISO 31000:2009 shows that the new version of the standard focuses more on the importance of senior management, strategic orientation, and fuller integration of risk management into the organization, including its transformation into an integral part of the decision-making process. Value creation is also given greater importance, which should be a major driver of risk management, and principles such as continuous improvement, stakeholder involvement, and consideration of human and cultural factors are used. As a result, the importance of feedback, including the exchange of information with the external environment, is increasing, and terminology terms have been moved to ISO Guide 73 Risk Management– a dictionary to facilitate the adoption of ISO 31000 by simplifying the language used therein to achieve a wider scope of application. It provides a better level of awareness when deciding on the strategic development of the organization, increases the level of operational efficiency and competitiveness, improves the market presence of the organization, and has a beneficial effect on expanding public support.

The implementation of a risk management system in an organization involves carrying out an analysis of known risks, as well as looking for ways to assess potential risks, predicting the extent of the damage they may cause to the organization in their eventual occurrence, and looking for ways to prevent them. The implementation of ISO 31000 creates a favorable infrastructure to address risks and benefit the organization, including neutralizing negative consequences. The managers may identify those events that would lead to risky situations, calculate the losses accompanying them in the event of manifestation, and determine appropriate precautions. An important feature is the fact that the effectiveness of risk management depends to a high extent on the implementation of meaningful communication and exchange of ideas in the organization, to have timeliness in getting everyone acquainted with possible emergencies, and to rely on appropriate behavior to deal with

them. The ISO 31000 standard enables the formalization of risk management practices in organizations, regardless of their subject matter, by implying systemic management to achieve better results.

2. Acknowledgement

Management is interpreted as a purposeful impact on a system. In strategic terms, it should support the long-term and sustainable development of organizations (Nikolaeva, 2018:225). This is closely related to risk.In the dynamic environment in which companies have to do their business today, risk management is one of the most complex factors, which is why its managers pay increasing attention. The presence of different types of risk implies knowledge of their specificities and finding appropriate approaches to them to avoid or at least minimize unintended consequences. In practice, risk can be seen as one of the drivers for strategic decision-making in organizations and may have a beneficial or negative impact. It is, therefore, necessary to correctly determine the overall level of risk in the organization. In general, the main prerequisite for the occurrence of risk is the uncertainty that accompanies unexpected changes in the environment. At the same time, the effectiveness of risk management requires compliance with specific principles as well as commensurately concerning the level of risk in the specific organization. It influences the size, quality, specificity of the activities carried out in the companies. The decisions to be taken depend on the specificities of the crisis. All this leads to the creation of a risk management template in organizations existing under the name ISO 31000. The implementation of ISO 31000 enables the development of an organizational risk management strategy to effectively identify risks, as well as find ways to reduce their impact on the organization. Overall, we should point out that ISO 31000 aims to build and develop an appropriate risk management culture, including control and monitoring. Risk situations require the readiness to process a large amount of information quickly, and the standard presents guidelines for integrating decision-making according to risk into management, planning, reporting, policies, organizational values, and culture. Risk management is also a prerequisite for achieving the sustainable development of organizations. Risk management should be an integrated part of the organizational culture of enterprises, it should transform strategic objectives into tactical and operational by implementing an effective policy by senior management. It is important for each organization today to be able to build up its smart risk management system, enabling the timely identification and analysis of risk situations, identifying the most important ones at any level of the organization, and taking adequate measures to address the losses they can lead to. Today, risk management should be seen as an integral part of managers' responsibility for the organizations they run. It focuses on creating effective economic protection for companies from undesirable effects that would cause them damage, so it must be systematic. The implementation of ISO 31000:2018 provides benefits for organizations by allowing them to analyze events that may lead to risks in the future, determine the damage they may inflict on them, specify precautionary measures, as well as actions in case of manifestation of risky situations that cannot be prevented. Risk management does not inherently avoid or eliminate risks but is aimed at realizing them, determining their likely impact in their manifestation, and, accordingly, how all this should be managed.

References

1. Fomichev, A. (2020). Risk management.
2. Georgiev, R. (2007). Delovi resheniya i sigurnost na organizatsiyata. Sofia
3. Gerunov, A. (2019). Risk Management: Typologies, Principles and Approaches. *Entrepreneurship*. Vol. VII. Issue: 2. pp. 205-244
4. Gerunov, A. (2020). Analysis and assessment of operational risks. *Economic and social alternatives*, No. 2, pp. 24-42 DOI: https://doi.org/10.37075/ISA.2020.2.03 [Online] Available

https://www.unwe.bg/doi/alternativi/2020.2/ISA.2020.2.03.pdf [Accessed 28/07/2021].
5. ISO 31000, Risk management. (2018). iso.org, Switzerland.
6. Ivanova, V. (2020). Environmental risk. Management and evaluation. *Management and Education* Vol. 16 (4). pp. 96-100
7. Lalonde, C., Boiral, O. (2012). Managing risks through ISO 31000: A critical analysis. *Risk Management* (2012) 14, 272 – 300. DOI: 10.1057/rm.2012.9
8. Krastev, D. (2020). Upravlenie pri krizi - komunikatsionni i informatsionni sistemi. Sofia: Snowmod
9. Kuznetsova, N. V. (2004). Upravlenie riskami. Vladivostok: Izdatelystvo Dalynevostochnogo universiteta.
10. Lecheva, I. (2020). Effectiveness and Efficiency in Risk Management. *Real Estate Property & Business*. 3:185-19. [Online] Available https://www.ceeol.com/search/article-detail?id=920417 [Accessed 28/07/2021].
11. Nikolaeva, V. (2018). Strategic Management of Business Organizations – Opportunities and Challenges. Izvestia Journal of the Union of Scientists – Varna. Economic Sciences Series, Vol. 7, №3, pp. 221-230
12. Neykova, R. (2013). The Role of the Risk Management for the Sustainable Development of the Industrial Enterprise. *Management and Sustainable Development*. Sofia: LTU, 1 (38), pp. 15-20
13. Proenca, D., Borbinha, J., Vieira, R. (2017). Risk Management: A Maturity Model based on ISO 31000. *Conference Paper*, July 2017. DOI: 10.1109/CBI.2017.40 [Online] Available https://www.researchgate.net/publication/319218604 [Accessed 09/06/2021].
14. Radulov, I., P. Andreeva. (2011). Predizvikatelstva pred upravlenieto na riska, kato chast ot menidzhmanta na sigurnostta. [Online] Available https://cio.bg/management/2011/05/16/3446837_predizvikatelstva_pred_upravlenieto_na_riska_kato/ [Accessed 09/06/2021].
15. Risk Management. (2017). [Online] Available https://arm953.wordpress.com/2017/02/20/%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5-%D0%BD%D0%B0-%D1%80%D0%B8%D1%81%D0%BA%D0%B0/ [Accessed 09/06/2021].
16. Risk management – Principles and guidelines. *Management du risque – Principes et lignes directrices*. (2009). International Standard ISO 31000. 2009, Switzerland
17. Standard Deviations – A Risk Practitioners Guide to ISO 31000 (2018). Institute of Risk Management. London
18. Stoev, St. (2017). Integration of Risk Management Processes into the Business of IT Companies. Izvestia, Journal of the Union of Scientists – Varna, "Economic Sciences" Series, 2/2017, pp. 225-233
19. Yordanova, D. (2020). About the intelligent risk management approach. Development of the Bulgarian and european economies – challenges and opportunities. Vol. 4 Collective Scientific Book of Faculty of Economics, "St. Cyril and St. Methodius" University of Veliko Tarnovo Annual Conference, held on 15.–16.10.2020 in Veliko Tarnovo. pp. 79-82
20. Zafirova, Tz. (2017). Strategichesko upravlenie. Varna: Izd. „Nauka i ikonomika", IU-Varna