Risk Management as an Instrument of the Effectiveness of Quality Management System

Petr REHACEK

Department of Systems Engineering, VSB, Technical University of Ostrava, Czech Republic; E-mail: perehacek@gmail.com

Abstract

The purpose of risk management is the creation and protection of value. It improves performance, encourages innovation and supports the achievement of objectives. Managing risk is iterative and assists organizations in setting strategy, achieving objectives and making informed decisions. Managing risk is part of governance and leadership, and is fundamental to how the organization is managed at all levels. It contributes to the improvement of management systems.

ISO 31000:2018 delivers a clearer guide that will help organizations use risk management principles to improve planning and make better decisions.

Keywords: consequence; event; likelihood; risk; stakeholder.

1. Introduction

The principles provide guidance on the characteristics of effective and efficient risk management, communicating its value and explaining its intention and purpose. The principles are the foundation for managing risk and should be considered when establishing the organization's risk management framework and processes. These principles should enable an organization to manage the effects of uncertainty on its objectives.

ISO 31000:2018 provides a risk management framework that supports all activities, including decision making across all levels of the organization:

- Review of the principles of risk management, which are the key criteria for its success;
- Focus on leadership by top management who should ensure that risk management is integrated into all organizational activities, starting with the governance of the organization;
- Greater emphasis on the iterative nature of risk management, drawing on new experiences, knowledge and analysis for the revision of process elements, actions and controls at each stage of the process;
- Streamlining of the content with greater focus on sustaining an open systems model that regularly exchanges feedback with its external environment to fit multiple needs and contexts.

Effective risk management requires the elements of Figure 1 and can be further explained as follows:

a) Integrated
Risk management is an integral part of all organizational activities.

b) Structured and comprehensive
Structured and comprehensive approach to risk management contributes to consistent and comparable results.

c) Customized
The risk management framework and process are customized and proportionate to the organization's external and internal context related to its objectives.

d) Inclusive
Appropriate and timely involvement of stakeholders enables their knowledge, views and perceptions to be considered. This results in improved awareness and informed risk management.

e) Dynamic
Risks can emerge, change or disappear as an organization's external and internal context changes. Risk management anticipates, detects, acknowledges and responds to those changes and events in an appropriate and timely manner.

f) Best available information
The inputs to risk management are based on historical and current information, as well as on future expectations. Risk management explicitly takes into account any limitations and uncertainties associated with such information and expectations. Information should be timely, clear and available to relevant stakeholders.
g) Human and cultural factors
Human behaviour and culture significantly influence all aspects of risk management at each level and stage.

h) Continual improvement
Risk management is continually improved through learning and experience.

2. Risk Management Process

The risk management process involves the systematic application of policies, procedures and practices to the activities of communicating and consulting, establishing the context and assessing, treating, monitoring, reviewing, recording and reporting risk. This process is illustrated in Figure 2.

![Figure 2. Risk Management Process](image)

The risk management process should be an integral part of management and decision-making and integrated into the structure, operations and processes of the organization. It can be applied at strategic, operational, programme or project levels. There can be many applications of the risk management process within an organization, customized to achieve objectives and to suit the external and internal context in which they are applied.

The dynamic and variable nature of human behaviour and culture should be considered throughout the risk management process. Although the risk management process is often presented as sequential, in practice it is iterative.

3. Communication and consultation

The purpose of communication and consultation is to assist relevant stakeholders in understanding risk, the basis on which decisions are made and the reasons why particular actions are required. Communication seeks to promote awareness and understanding of risk, whereas consultation involves obtaining feedback and information to support decision-making. Close coordination between the two should facilitate factual, timely, relevant, accurate and understandable exchange of information, taking into account the confidentiality and integrity of information as well as the privacy rights of individuals. Communication and consultation with appropriate external and internal stakeholders should take place within and throughout all steps of the risk management process (Verbonco and Mihai, 2016).

Communication and consultation aims to:
- bring different areas of expertise together for each step of the risk management process;
- ensure that different views are appropriately considered when defining risk criteria and when evaluating risks;
- provide sufficient information to facilitate risk oversight and decision-making;
- build a sense of inclusiveness and ownership among those affected by risk.

4. Scope, context and criteria

The purpose of establishing the scope, the context and criteria is to customize the risk management process, enabling effective risk assessment and appropriate risk treatment. Scope, context and criteria involve defining the scope of the process, and understanding the external and internal context.

4.1. Defining the scope

The organization should define the scope of its risk management activities. As the risk management process may be applied at different levels (e.g. strategic, operational, programme, project, or other activities), it is important to be clear about the scope under consideration, the relevant objectives to be considered and their alignment with organizational objectives. When planning the approach, considerations include:
- objectives and decisions that need to be made;
- outcomes expected from the steps to be taken in the process;
- time, location, specific inclusions and exclusions;
- appropriate risk assessment tools and techniques;
- resources required, responsibilities and records to be kept;
- relationships with other projects, processes and activities.

4.2. External and internal context

The external and internal context is the environment in which the organization seeks to define and achieve its objectives. The context of the risk management process should be established from the understanding of the external and internal environment in which the organization operates and should reflect the specific environment of the activity to which the risk management process is to be applied.

Understanding the context is important because:
- risk management takes place in the context of the objectives and activities of the organization;
- organizational factors can be a source of risk;
- the purpose and scope of the risk management process may be interrelated with the objectives of the organization as a whole.

4.3. Defining risk criteria

The organization should specify the amount and type of risk that it may or may not take, relative to objectives. It should also define criteria to evaluate the significance of risk and to support decision-making processes. Risk criteria should be aligned with the risk management framework and customized to the specific purpose and scope of the activity under consideration. Risk criteria should reflect the organization's values, objectives and resources and be consistent with policies and statements about risk management. The criteria should be defined taking into consideration the organization's obligations and the views of stakeholders.

While risk criteria should be established at the beginning of the risk assessment process, they are dynamic and should be continually reviewed and amended, if necessary.
To set risk criteria, the following should be considered:

- the nature and type of uncertainties that can affect outcomes and objectives (both tangible and intangible);
- how consequences (both positive and negative) and likelihood will be defined and measured;
- time-related factors;
- consistency in the use of measurements;
- how the level of risk is to be determined;
- how combinations and sequences of multiple risks will be taken into account;
- the organization’s capacity.

5. Risk assessment

Risk assessment is the overall process of risk identification, risk analysis and risk evaluation. Risk assessment should be conducted systematically, iteratively and collaboratively, drawing on the knowledge and views of stakeholders. It should use the best available information, supplemented by further enquiry as necessary.

5.1. Risk identification

The purpose of risk identification is to find, recognize and describe risks that might help or prevent an organization achieving its objectives. Relevant, appropriate and up-to-date information is important in identifying risks (Kerekes and Csernátoni, 2016).

The organization can use a range of techniques for identifying uncertainties that may affect one or more objectives. The following factors, and the relationship between these factors, should be considered:

- tangible and intangible sources of risk;
- causes and events;
- threats and opportunities;
- vulnerabilities and capabilities;
- changes in the external and internal context;
- indicators of emerging risks;
- the nature and value of assets and resources;
- consequences and their impact on objectives;
- limitations of knowledge and reliability of information;
- time-related factors;
- biases, assumptions and beliefs of those involved.

The organization should identify risks, whether or not their sources are under its control. Consideration should be given that there may be more than one type of outcome, which may result in a variety of tangible or intangible consequences.

5.2. Risk analysis

The purpose of risk analysis is to comprehend the nature of risk and its characteristics including, where appropriate, the level of risk. Risk analysis involves a detailed consideration of uncertainties, risk sources, consequences, likelihood, events, scenarios, controls and their effectiveness. An event can have multiple causes and consequences and can affect multiple objectives (Diana, Mirela and Sorin, 2017).

Risk analysis can be undertaken with varying degrees of detail and complexity, depending on the purpose of the analysis, the availability and reliability of information, and the resources available. Analysis techniques can be qualitative, quantitative or a combination of these, depending on the circumstances and intended use.

Risk analysis should consider factors such as:

- the likelihood of events and consequences;
- the nature and magnitude of consequences;
- complexity and connectivity;
- time-related factors and volatility;
- the effectiveness of existing controls;
- sensitivity and confidence levels.

The risk analysis may be influenced by any divergence of opinions, biases, perceptions of risk and judgements. Additional influences are the quality of the information used, the assumptions and exclusions made, any limitations of the techniques and how they are executed. These influences should be considered, documented and communicated to decision makers.

Highly uncertain events can be difficult to quantify. This can be an issue when analysing events with severe consequences. In such cases, using a combination of techniques generally provides greater insight.

Risk analysis provides an input to risk evaluation, to decisions on whether risk needs to be treated and how, and on the most appropriate risk treatment strategy and methods. The results provide insight for decisions, where choices are being made, and the options involve different types and levels of risk.

5.3. Risk evaluation

The purpose of risk evaluation is to support decisions. Risk evaluation involves comparing the results of the risk analysis with the established risk criteria to determine where additional action is required. This can lead to a decision to:

- do nothing further;
- consider risk treatment options;
- undertake further analysis to better understand the risk;
- maintain existing controls;
- reconsider objectives.

Decisions should take account of the wider context and the actual and perceived consequences to external and internal stakeholders.

The outcome of risk evaluation should be recorded, communicated and then validated at appropriate levels of the organization.

6. Risk treatment

The purpose of risk treatment is to select and implement options for addressing risk.

Risk treatment involves an iterative process of:

- formulating and selecting risk treatment options;
- planning and implementing risk treatment;
- assessing the effectiveness of that treatment;
- deciding whether the remaining risk is acceptable;
- if not acceptable, taking further treatment.

6.1. Selection of risk treatment options

Selecting the most appropriate risk treatment option(s) involves balancing the potential benefits derived in relation to the achievement of the objectives against costs, effort or disadvantages of implementation.

Risk treatment options are not necessarily mutually exclusive or appropriate in all circumstances. Options for treating risk may involve one or more of the following:

- avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;
- taking or increasing the risk in order to pursue an opportunity;
- removing the risk source;
- changing the likelihood;
- changing the consequences;
- sharing the risk (e.g. through contracts, buying insurance);
retaining the risk by informed decision.

Justification for risk treatment is broader than solely economic considerations and should take into account all of the organization's obligations, voluntary commitments and stakeholder views. The selection of risk treatment options should be made in accordance with the organization's objectives, risk criteria and available resources.

When selecting risk treatment options, the organization should consider the values, perceptions and potential involvement of stakeholders and the most appropriate ways to communicate and consult with them. Though equally effective, some risk treatments can be more acceptable to some stakeholders than to others.

Risk treatments, even if carefully designed and implemented might not produce the expected outcomes and could produce unintended consequences. Monitoring and review need to be an integral part of the risk treatment implementation to give assurance that the different forms of treatment become and remain effective.

Risk treatment can also introduce new risks that need to be managed. If there are no treatment options available or if treatment options do not sufficiently modify the risk, the risk should be recorded and kept under ongoing review.

Decision makers and other stakeholders should be aware of the nature and extent of the remaining risk after risk treatment. The remaining risk should be documented and subjected to monitoring, review and, where appropriate, further treatment.

6.2. Preparing and implementing risk treatment plans

The purpose of risk treatment plans is to specify how the chosen treatment options will be implemented, so that arrangements are understood by those involved, and progress against the plan can be monitored. The treatment plan should clearly identify the order in which risk treatment should be implemented.

Treatment plans should be integrated into the management plans and processes of the organization, in consultation with appropriate stakeholders.

The information provided in the treatment plan should include:

- the rationale for selection of the treatment options, including the expected benefits to be gained;
- those who are accountable and responsible for approving and implementing the plan;
- the proposed actions;
- the resources required, including contingencies;
- the performance measures;
- the constraints;
- the required reporting and monitoring;
- when actions are expected to be undertaken and completed.

7. Monitoring and review

The purpose of monitoring and review is to assure and improve the quality and effectiveness of process design, implementation and outcomes. Ongoing monitoring and periodic review of the risk management process and its outcomes should be a planned part of the risk management process, with responsibilities clearly defined. Monitoring and review should take place in all stages of the process. Monitoring and review includes planning, gathering and analysing information, recording results and providing feedback. The results of monitoring and review should be incorporated throughout the organization's performance management, measurement and reporting activities.

8. Recording and reporting

The risk management process and its outcomes should be documented and reported through appropriate mechanisms. Recording and reporting aims to:

- communicate risk management activities and outcomes across the organization;
- provide information for decision-making;
- improve risk management activities;
- assist interaction with stakeholders, including those with responsibility and accountability for risk management activities.

Decisions concerning the creation, retention and handling of documented information should take into account, but not be limited to: their use, information sensitivity and the external and internal context.

Reporting is an integral part of the organization's governance and should enhance the quality of dialogue with stakeholders and support top management and oversight bodies in meeting their responsibilities.

Factors to consider for reporting include, but are not limited to:

- differing stakeholders and their specific information needs and requirements;
- cost, frequency and timeliness of reporting;
- method of reporting;
- relevance of information to organizational objectives and decision-making.

9. Conclusions

Based on this article we can understand risk management as the "effect of uncertainty on objectives", which focuses on the effect of incomplete knowledge of events or circumstances on an organization's decision making. This requires a change in the traditional understanding of risk, forcing organizations to tailor risk management to their needs and objectives. A risk management has an influence on all activities in organisation, including decision-making across all levels of the organization. A risk management and its processes should be integrated with management systems to ensure consistency and effectiveness of management control across all areas of the organization. This would include strategy and planning, organizational resilience, IT, corporate governance, HR, compliance, quality, health and safety, business continuity, crisis management and security.

References