21st International Conference Man and Working Environment
SEMSIE
Safety Engineering & Management – Science, Industry, Education

REVIEW PAPER

DOI: 10.46793/SEMSIE25.213J

KATARINA JANKOVIĆ[1]
MILICA MLADENOVIĆ[2]
NENAD KOMAZEC[3]

[1]University of Defence, Military Academy, Belgrade, Serbia
[2, 3]Regional Association for Security and Crisis Management (RASEC), Belgrade, Serbia

[1]jankovickatarina95@gmail.com
[2] mladenovicmilica21@yahoo.com
[3]nenadkomazec@yahoo.com

RISK MANAGEMENT IN EMERGENCIES: REDUCING VULNERABILITY OF PEOPLE AND ASSETS

Abstract: *Businesses function within a dynamic context, frequently facing negative events and challenges. Modern business processes highlight the need for managing emergency events under conditions of uncertainty. Uncertainty is directly related to risk. Risk management within the field of crisis management is primarily focused on identifying risks and implementing measures for their treatment. Different risk theorists offer various approaches to defining risk and the phases of risk management. The risk management process encompasses a wide range of activities carried out in specific phases, requiring the exploration of opportunities for developing and implementing a systematic approach. Different business systems have different technological processes, but the risk management process is based on the same foundation. Maintaining the quality of the system is directly dependent on the organization of risk management activities related to emergency events. The objective of this process is to reduce the vulnerability of people and material assets through the implementation of preventive and reactive measures.*

Keywords: risk management, risk, risk management, organizational systems

ORCID iDs: Katarina Janković https://orcid.org/0009-0006-0988-4895
Milica Mladenović https://orcid.org/0000-0002-8301-0452
Nenad Komazec https://orcid.org/0000-0001-9227-118X

INTRODUCTION

The modern era has made the causes of adverse events increasingly complex and their consequences more destructive. In order to prevent such events or mitigate their consequences, prevention must be integrated into all phases of the event's development. It is a fact that various safety systems exist within business systems, such as occupational health and safety systems, fire protection systems, physical security, and others. Each of these systems plays its own role in the collective mosaic of corporate security. The key factor for successfully implementing security functions—both individually and collectively—is the knowledge of all individuals involved in the management process. This knowledge is not limited to security topics but also includes all managerial elements.

Since organizational security is a crucial function that encompasses or permeates all aspects of organizational management, it is essential to identify all factors that influence the occurrence and development of events with negative impacts. A modern tool that allows systematic monitoring of such events, assessing the likelihood of their occurrence, and taking preventive measures is risk assessment. Risk assessment directly depends on the level of knowledge of the individuals involved in a process, as well as their understanding of the process itself and external factors.

All risks have a direct or indirect impact on key business processes, which are primarily conditioned by the core dimensions of the organization. They manifest through complexity, formalization, and centralization, and are especially pronounced in organizations where centralization is the dominant element. Risk is always relevant, variable, and dynamic, which makes risk management a pervasive and process-based activity.

RISK AND EMERGENCY EVENTS

Risk is inherent in all business processes. In its broadest and most general conceptual definition, risk is described as the possibility of suffering harm or loss, or as a "factor, object, element, or course involving uncertainty and danger." However, the concept of risk not only evolves over time but also varies depending on the activity in which it is being analyzed, and as such, it is defined and assessed differently. Two main meanings of risk can be distinguished:

1. The possibility that an action or activity will result in damage or loss to materials or persons.
2. The term "risk" is used when outcomes are uncertain (Beck, 1999).

The existence of risk involves uncertainty, which is linked to a lack of information or knowledge, or to the assumption of other, even positive, outcomes. Existing definitions of risk characterize it as the potential for an undesirable event to occur, resulting in various types of negative consequences. The term *possibility* holds a

central place, as it implies uncertainty about the outcome of an event, making the presence of risk directly tied to uncertainty. Since complete certainty is rarely achievable, risk and uncertainty are considered integral parts of most business processes. Uncertainty arises when the future is unknown, and there are no actual (objective or subjective) probabilities associated with alternative outcomes. Risk occurs when specific numerical data about the probabilities are associated with alternative outcomes.

Events with negative impacts are the focus of modern business processes. A changing environment generates a range of events, with or without negative consequences. Monitoring environmental changes is one of the primary challenges of contemporary business processes, particularly in terms of obtaining the information necessary for managing those changes. Events are consequences of a set of environmental circumstances. An event is defined as a circumstance that occurs without the involvement of the organization's will, but which objectively causes the emergence, cessation, or alteration of a state. Events are often referred to as acts of force majeure. Based on this definition, several characteristics can be identified (Kekovic and Kesetovic, 2007; Cvetkovic, 2006):

- An event may consist of one or more occurrences and may have multiple causes;
- An event may consist of something that did not happen;
- An event may sometimes be classified as an "incident" or an "accident";
- An event without consequences may also be considered an event that was "barely avoided," "almost occurred," or was a "near miss."

These characteristics point to the existence of uncertainty and the need to act at the boundaries of our understanding of circumstances. The magnitude and frequency of a set of circumstances are determined by a combination of different environmental factors, which also represent sources of risk (Cvetkovic, 2006). These factors do not influence outcomes in a uniform manner in terms of time, space, and intensity; thus, their significance varies. All factors that can cause a negative event can be classified into four groups: the human factor, the technical-technological factor, the natural factor, and the social factor.

Based on the above, it can be concluded that any event that actually or hypothetically implies negative consequences represents an emergency event. Reducing the impact, preventing, or avoiding a negative event is the focus of the emergency event prevention process (Vauglan, 1997). The "emergency" nature of an event refers to an unplanned occurrence, an unexpected action, or a deviation from normal operations. Organizational management monitors environmental changes, analyzes them, and identifies those that are actually or potentially hazardous to the organization. Identification itself depends on the level of understanding of the characteristics of phenomena that occur or may occur. The subsequent hazard analysis phase will produce poor results if the identification process is based on inadequate information (Molak, 2007).

THE PROCESS-ORIENTED NATURE OF RISK MANAGEMENT

The dynamic environment in which business processes operate generates changes that often produce negative effects on the system. Business requirements and objectives are defined in a way that their fulfillment justifies the system's existence. The desired state of the system is defined through the established quality, which represents the degree to which a set of inherent characteristics meets the requirements. These requirements are defined as needs or expectations that are either implicit or mandatory, and they are materialized through business goals. Responsibility for achieving these objectives lies with the manager, and consequently, so does the responsibility for the quality of the system's functioning.

A prerequisite for the successful implementation and sustainability of the risk management process is its integration into the general process of business management and full support from the management. Risk management must be integrated at all levels of business process management and across all specific areas of organizational operations. A process-oriented approach to risk management enables the proper processing of all risk-related information generated within a given time unit and its use in the decision-making process.

In a decentralized concept, the degree of decentralization depends on the level of responsibility distribution in risk management. In such structures, risk assessment teams exist within each area, particularly characteristic of production-oriented organizations. These teams usually consist of representatives from the following functions and departments: marketing, production, technology, procurement, quality control, and sales. If needed, the team is expanded to include members from other departments such as logistics, after-sales, legal, etc. These teams are both the assessors and the bearers of responsibility for risk. Within these teams, a team leader must be defined, who also serves as a member of the main risk management team.

The application and implementation of the risk management process in business processes require the full commitment of management to the process. It is also essential for all actors involved in the technological and work processes to participate in risk management. Of particular importance are individuals from the governing structures who manage risks within their areas. Overall risk is managed by top management.

To ensure the optimal implementation and realization of the risk management process, the process should:

- Define, align with higher-level management, and approve a risk management policy;

- Inform all stakeholders about the decision to apply risk management and what is expected of them;
- Define indicators for the successful achievement of risk management system objectives;
- Ensure that the objectives of risk management are complementary to the organizational goals;
- Ensure compliance with legal regulations; and
- Provide the necessary resources for the realization of the risk management process.

Uncertainty exists in all business process activities. The top manager, as the decision-maker, bears full responsibility for the quality and execution of the decision and assumes the associated risk. When there is a lack of information necessary for decision-making, this implies a need to gather the missing data. The time between recognizing the lack of information and obtaining it contributes to increased uncertainty and insecurity. The obtained information may contribute to reducing uncertainty, but it does not necessarily eliminate it.

SYSTEMIC APPROACH TO RISK MANAGEMENT

The risk management system consists of two elements: the object of management and the subject of management. The object of management is the risk, observed in the context of the hazards being analyzed. The subject of management is a specially trained and appropriately authorized decision-maker—either an individual or a team—who, through the application of various tools and methods, performs the risk management function.

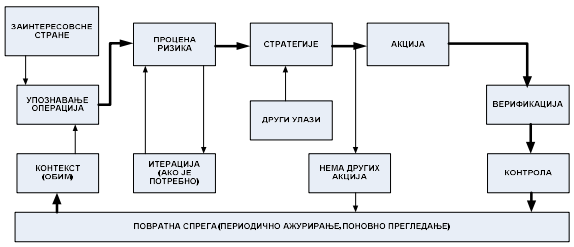

Figure 1. *Phases of Risk Management (Source: Savic, Stankovic, 2018)*

A systemic approach enables the observation of all internal and external connections between the actors within the risk management system, their integration with organizational processes, and the degree of contribution to achieving organizational goals. Organizational mechanisms within risk management systems must be capable of recognizing new problems, creating and implementing new solutions (decisions), ensuring maximum concentration and availability of resources, consolidating existing capacities, and mobilizing forces—all with the aim of mitigating the consequences of a risk event in the shortest possible time.

Within the structure of the risk management system, two mutually exclusive principles are implemented: the principle of individual management (unity of authority and responsibility) and the principle of the distribution of authority and responsibility.

Table 1. Characteristics of Risk Management According to Different Definitions

Source	Elements of Definitions	Common Characteristics
Vauglan E.J.	Maintaining system quality even when risk events occur	Risk management is a part of organizational processes. Risk management is an integral part of the quality system It supports decision-making. It includes risk identification, measurement, analysis, and monitoring.
AS/NZS	Balancing gains and losses	
Sage A.	Controlling areas and events that are potential triggers of unwanted changes	
RMPS	Comprehensive decision-support process integrated through quality	
ISO 31000	Structured process of risk identification, measurement, treatment, and monitoring	

Although every risk management strategy depends on the nature of the system it addresses, the processes described are continuous and logically connected, forming a unified process of the systemic approach to risk management. These processes include: risk planning, risk assessment, and the implementation of risk mitigation measures.

Risk planning as a function of systemic prevention

Every management process begins with planning, which can be defined as the process of setting future goals, making assumptions about the environment in which these goals should be achieved, and choosing a course of action, resources, and methods for achieving those goals. Planning involves analyzing the environment and the organization's capabilities in a changing context, assessing total potential, strengths and weaknesses, alternative development paths, and more. Planning here does not refer strictly to formal short-term and long-term plans, but rather to the organization's long-term strategic orientation. This includes diagnosing the security environment, determining courses of action, setting goals to be achieved, selecting the strategy for achieving those goals, and making managerial decisions through all phases.

Since all other management functions are aligned in the planning process with the selected goals and objectives, the responsibility of the managers performing this function becomes clear. Planning is an integral part of

management at all levels, but its scope differs depending on the level of managerial authority.

Planning is the fundamental starting function of management. It is a process that includes task and goal selection, defining actions to achieve them, and making decisions—i.e., choosing between alternative future courses of action. Plans ensure a rational approach to achieving previously selected goals.

Risk planning is the initial phase of risk management and consists of a set of actions implemented throughout the entire risk management process, as defined by the risk management plan. It includes: defining the problem context and project scope, and familiarization with operations. All stakeholders should be involved in risk planning.

The core elements of a risk management plan are:

- A summary of the system: vision, mission, objectives and system purpose, required standards, and development strategy;
- The approach to risk: methods for risk assessment, risk determination, scales for risk ranking;
- The organization of the risk management process through its phases;
- Responsibility for risk management.

The risk management plan serves as the foundation and guideline for the risk management team.

Risk planning as a function of systemic prevention

The efficiency and effectiveness of the risk management process can only be maximized through continuous improvement. Organizational systems must develop the capacity for risk management. The fundamental assumption for this capacity is the existence of a risk management system, that the decision-maker understands and accepts the need for risk management, that all actors in the process are aware of their obligations within risk management, and that there are qualified personnel competent in implementing and supervising the process. Risk management holds critical importance for the functioning of organizational systems, and therefore, the implementation of ISO 31000 is necessary in the risk management process.

According to this standard, the key components for improving the risk management process are:

1. Continuous development of the risk management system. All elements of the risk management system must be subject to ongoing development. By setting clear performance indicators, organizations can measure the effectiveness of both the organization and individuals responsible for risk management. System reviews should be conducted annually, or more frequently if necessary, to incorporate new goals and adjust existing ones. The assessment of the properties of the risk management system is an integral part of evaluating the effectiveness of organizational systems.
2. Clearly defined and fully accepted accountability for risks, risk control, and implementation of the risk treatment plan
   This means that a risk management policy defines the direction and principles for applying the risk management process in the organization, and internal regulations and procedures define the risk management system. The core of the risk management system lies in human resources—trained and capable of implementing, developing, and supervising the risk management process. With the necessary capacity and resources, management actions can control and improve the process, monitor risks, and communicate effectively about risks—internally with management and externally with stakeholders. Organizational systems use internal regulations to place all risk management actors in a dependent position to ensure compliance with obligations defined by the organization's decision-makers.
3. Inclusion of risk in every decision-making process within the organization
   Regardless of the level of importance, every decision must take into account the risks and apply risk management to an appropriate level. This means that decisions, as driving mechanisms in organizational systems, should be based on conclusions derived from risk management system analysis. These decisions, correlated with the management system of the organization and the products of the risk management process, allow for comprehensive consideration of all aspects of potentially risky events.
4. Permanent communication about risk as part of the organizational system management
5. Establishing the risk management process as a central management process
   This ensures the evaluation of its direct impact on planned objectives.

By continuously respecting these improvement components, the conditions are created for effective and efficient implementation of the risk management system at all levels of business process management.

CONCLUSION

Everyday business operations, in their entirety, take place under certain conditions of uncertainty. The measure of this uncertainty is risk. This observation highlights the importance of risk management in minimizing the impact and consequences of specific undesirable situations. Risk management is a process of actively making decisions to avoid problems—or at least to influence their consequences and likelihood—before they occur. The decision-making process takes place in risk-laden situations and under uncertainty, which essentially presents a challenge for those in managerial roles.

Risk management directly improves the decision-making process, especially for high-risk decisions, by enabling managers to understand the environment (both

internal and external), recognize risks, protect themselves and the organization, and thereby achieve their objectives. In this context, the article seeks to address possible approaches to managing specific risks based on a systemic foundation, contributing to risk management as a vital management function. Anticipating events that may unfold uncontrollably is becoming a daily activity, and risk management is becoming an equal process alongside design, production, service delivery, etc. On the other hand, risk management should ensure the continuous operation of the system. Documentation generated through the risk management process enables the accreditation and authorization of the risk management process itself.

What is common to all forms of risk management is its defined role as a decision-making tool, integrating continuous assessment of what might go wrong (risks), determining which risks are most significant, and developing and applying strategies to address them. Based on the above—especially in the context of risk analysis and management—the key elements of risk management can be identified as: identification, analysis, planning, research, control, and communication. These elements are integrated and interconnected, forming a logical sequence in the risk management process.

Risk management is a fundamental tool for the prevention of emergency events. A reduced number of negative events implies fewer consequences for the business system, which in turn leads to an increase in system quality. By establishing such a process, continuous improvement in the quality of the business system is ensured.

REFERENCE

Bek, U. (2001), Rizično društvo, Filip Višnjić, Beograd

Beck U. (1999), World risk society, Cambridge, Polity Press

Vauglan, E.,J.(1997) Risk management, John Willie & Sons, New York

Kekovic, Z., Kesetovic, Z. (2007) Hrestomatija-prevencija krize, Fakultet bezbednosti, Beograd

Cvetkovic, D. (2006), Upravljanje rizicima, clanak, Festival kvaliteta, Kragujevac

Molak B, (2007), Sta je upravljanje krizama, clanak, Zagreb
Standard ISO 31000:2018

ISO TC 223/SC, Internacionalni standard za društvenu sigurnost

Cupic, M., Tumala, V.M. (1997), Savremeno odlucivanje, metoda i primena, FON, Beograd, 1997.

Jankovic, K., Komazec, N. (2019), Uticaj edukacije u oblasti procene rizika na prevenciju vanrednih dogadjaja, Međunarodna konferencija Rizik i bezbednosni inzenjering, Kopaonik

Savic, S., Stankovic, M. (2012). Teorija sistema i rizika. Beograd: Akademska misao