10th INTERNATIONAL SCIENTIFIC CONFERENCE
ON DEFENSIVE TECHNOLOGIES
OTEH 2022
Belgrade, Serbia, 13 – 14 October 2022

RISK MANAGEMENT AT PUBLIC COMPANY „NUCLEAR FACILITIES OF SERBIA“

BOJAN RADOŠ
PC „Nuclear Facilities of Serbia“, Mike Petrovića Alasa 12-14, Vinča, Belgrade
+381628869090, bojan.rados@nuklearniobjekti.rs

NATAŠA LAZAREVIĆ
PC „Nuclear Facilities of Serbia“, Mike Petrovića Alasa 12-14, Vinča, Belgrade
+381628869118, natasa.lazarevic@nuklearniobjekti.rs

JOVANA KNEŽEVIĆ
PC „Nuclear Facilities of Serbia“, Mike Petrovića Alasa 12-14, Vinča, Belgrade
+381628869113, jovana.knezevic@nuklearniobjekti.rs

DALIBOR ARBUTINA
PC „Nuclear Facilities of Serbia“, Mike Petrovića Alasa 12-14, Vinča, Belgrade
+381628869007, dalibor.arbutina@nuklearniobjekti.rs

Abstract: *Public Company "Nuclear Facilities of Serbia" has an established risk management system. This system is designed to reflect the regulatory requirements related to the financial management and control system, as well as the requirements related to the standards SRPS ISO 9001:2015 and SRPS ISO/IEC 17025:2017 regarding the actions to address risks and opportunities. The adequacy of the established system corresponds to the complexity and activities of the company as the only nuclear operator in the country, taking into account the concept of risk-based thinking, risk analysis and preventive actions which are components of planning and implementation of nuclear facilities management activities. The efficiency of the risk management system ensures that the company's risk profile is in accordance with the established level of risk acceptance, which is confirmed by appropriate certification and accreditation. This paper presents the methodology of risk management in PC "Nuclear Facilities of Serbia" with challenges to improve and support business strategy and development.*

Keywords: *risk, control, management, information, organization.*

1. INTRODUCTION

The main and highest risk in the work of the Public Company of "Nuclear Facilities of Serbia" is the occurrence of a radiological or nuclear emergency during the management of nuclear facilities. A radiological or nuclear emergency may be the result of regular activities, but also of diversion, sabotage and terrorist attack.
All activities are performed at a high quality level of radiation and nuclear safety and security, with a constant emphasis on their improvement, and in accordance with the licenses and authorizations issued by the regulatory body and the established quality management system according to the standards SRPS ISO/IEC 17025:2017 and SRPS ISO 9001:2015, trained staff and available resources[1].

An integral part of the quality management system is the risk management process. This process is designed to identify potential risk events that can affect the business, then to respond to the identified risks through the system of internal controls, as well as to communicate and supervise the risks.

All activities are planned, taking into account the risk and the obligation to reduce it to the lowest possible level, which is made possible by the implementation of measures in each business process [2].

The entire process of risk management is supported by the established system of financial management and control, which is a regulatory requirement and consists of a set of adopted strategies, policies, procedures and activities that provide reasonable assurance that the goals of the long-term and medium-term plan of the business strategy and development of the company can be to achieve in a proper, economical, efficient and effective way [3].

2. RISK MANAGEMENT PROCESS

According to its characteristics, system of risk management is designed to be continuous in its application and to refer to the entire internal organization, work resources and human resources in the company. The system includes two key and strategic documents that define the entire risk management process: Risk Management Strategy and Methodology for identifying, measuring, communicating and monitoring risks.

The risk management strategy defines the structure of the risk management process, which consists of four sub-processes that maintain their interdependence of functioning: risk assessment, risk treatment, risk communication and risk supervision. In addition, content of appendix of this document shows risks to which business processes are exposed and which represent the context of understanding the environment and internal organization of work processes [4].

The methodology for identifying, measuring, communicating and monitoring risks defines the procedures for managing the aforementioned structure of the risk management process [5].

These documents are reviewed periodically in terms of effectiveness, as well as in situations where there are significant changes related to the component of the control environment of the COSO (Committee of Sponsoring Organizations of the Treadway Commission) system of internal controls, which the company applies as a regulatory requirement of the system of the financial management and control.

2.1. Risk assessment

Risk assessment includes three sub-processes: identification, analysis and classification of risks.

The risk identification proceeding is carried out in relation to the created Map of Business Processes, which provides an overview of all processes and sub-processes that are defined by the Rulebook on the Organization and systematization of work in the company. Risk identification is focused on data collection in order to determine the types of risks to which the processes and sub-processes from the Business Process Map are exposed. In addition to the type of risk, the sources of risk are also defined, which can be: intentional or accidental error, mechanical execution of activities, inexperience or insufficient number of executors, and force majeure. The process of identifying the type of risk as well as the source of risk is carried out by managers of organizational units in the form of self-assessment, since managers know best the business processes they manage and can most objectively comment on which risk the business process is exposed to [6].

As part of the risk analysis, each risk is considered in relation to its components: the impact of the risk, the likelihood of the realization of the risk event, the vulnerability to the risk event and the speed of the realization of the risk. The basis of the risk analysis proceeding is the assignment of a weight value that expresses the significance of that risk in relation to its components. The weighting values assigned represent the significance of the risk component to which business processes are exposed in the execution of their activities. Each weight in relation to its given description corresponding to the significance of the risk, which can be of no significance, low, medium, high or extreme risk is expressed in relation to its assigned numerical value on the weight value scale.

The values on the weighting scale are in the range from 1-5. By selecting weights per component and multiplying them, the measured risk value per process is obtained. Each assigned weighting value is presented in its descriptive form. The descriptive description is designed to specify the situation that corresponds to the assigned weighting level. Based on the assigned values, the significance of the risk components on the realization of the risky event is determined. The risk calculation procedure itself primarily boils down to the multiplication of the risk impact component and the likelihood of the realization of the risky event. In this way, the inherent value of the risk is expressed without the application of control activities that serve to mitigate its value.

The risk impact component has a dominant importance, because it is the one that shows what can happen with the realization of a risky event and what its consequences are. On the other hand, the likelihood of realization is a key component, because whether a risky event can happen and how often, it determines the character of the risk as well as the internal controls that are applied to mitigate the impact of such a risky event.

An example of the description of the value for the likelihood of the realization of a risk event of high risk significance is given in table 1. An example of the description of the significance of a high risk in relation to its weighting value according to the risk impact component is given in table 2.

Table 1. Risk component - The likelihood of occurrence of a risk event of a high level of significance

Weight value	Description of Likelihood	Time Frame
4	It is likely that the event will come occure	Event will happened once per 6 months

Table 2. Risk component – Impact of risk

Weight value	Description of criteria
High level of significance	Absence of control mechanisms and activities that can have a material impact on the execution of business process activities.
	There is an outflow of professional personnel, which causes a decrease in the effectiveness of control activities.
	Risk event prevention and detection mechanisms have shortcomings that may miss signaling events that have a material impact on human and material resources.
	The resulting failures in business have a materially significant impact and cannot be covered from the Financial result/Capital.
	Absence of reputational risk management mechanisms due to which attention-grabbing information can flow unchecked.

By calculating the inherent risk value, the need to introduce internal controls is determined, especially if the exposure is materially significant. The amount of the costs of introducing controls can be in the maximum amount of consequences that a risky event can bring if it

is realized. The introduced control and verification of its effectiveness should result in a residual risk that corresponds to the defined level of acceptable risk.

Beside to this, another model is used that takes into consideration the impact and vulnerability on the risk event, if this determinant determines the value of the risk more precisely. This risk calculation proceeding is applied at the level of each sub-process and organizational unit process within the Business Process Map. Since each process can be exposed to more risks, the one that has the greatest material impact on the realization of the risky event and its consequences for the business is taken into consideration. The measured risk values can range from 1-25 weighting points. Depending on the obtained values of the measured risks, their importance is determined, i.e. risk classification. Based on the measured significance of the risk, it is determined which risks have priority in their monitoring and action according to prevention measures.

The calculated risk value per business process is considered in relation to the Risk Measurement Matrix according to Table 3, as well as in relation to the defined clusters of obtained weighting points that determine the importance of risks and their consideration priority in relation to supervision and action according to prevention measures according to Table 4.

Depending on the selected weight per risk component, its measured value depends, as well as the classification of the significance of such measured risks. The value of the measured risk is a function of the assigned weighting values for the risk components.

Table 3. Risk Measurement Matrix

	Likelihood				
Impact	1	2	3	4	5
	2	4	6	8	10
	3	6	9	12	15
	4	8	12	16	20
	5	10	15	20	25

Table 4. Risk significance of business processes

1-5	6-10	11-15	16-20	21-25
No significance	Low risk	Medium risk	High risk	Extreme risk

Those business processes whose significance has been determined at the level of high or extreme level of risk significance have priority in consideration. These processes form the basis for consideration of the risk treatment procedure and creation of the Risk Register.

Since the process of risk management is by its nature continuous, analyzes of the measured significance of risks are performed periodically. These considerations for business processes are constantly applied, because the measured values are not constant over the time and can change according to their significance and priorities for action. These changes can occur due to changes in the business environment as well as changes in the work process itself. For this reason, the data collection procedure is carried out through a quarterly questionnaire on realized risk events at the level of organizational units.

This questionnaire is made up of assumed risk events that can have an impact on business processes. In the questionnaire, it is stated whether any of the risky events took place, along with a description of the risky event, what specifically happened and what consequences resulted from the realization of the risky event. For each listed risk event, data is entered as to whether its realization resulted in material or monetary damage, as well as the type of risk associated with such a risk event.

The questionnaire is also an instrument of communication about risks, as it takes into account the corrective measures taken in order to mitigate its effects, as well as reporting on the state of the risk management system. In this way reported risk events it can be seen the scenarios of the realization of the events, their frequency of realization, the source of the risky events as well as the location of its realization concerning the specific organizational unit and the business process that is subject to its realization.

Based on the questionnaire in which the data on realized risk events and the Risk Register are entered, it is determined through self-assessment whether the significance of the risk has remained at the same reference values during the period or whether there have been changes. All resulting changes are recorded in the Map of business processes. In this way, the updating of the Map of business processes and current values of the significance of risks is ensured.

2.2. Risk treatment

The risk treatment proceeding aims to show in which way will be resolved the question of materially most important risks. In this regars there is four available options to take into consideration: risk acceptance, risk avoidance, risk mitigation and risk transfer. Which option will be chosen depends on each individually identified materially significant risk.

Within the proceeding of risk treatment, the following activities are carried out: designing a map of the interaction of risks and risk events, creating a risk register and determining which risks are prioritized for consideration and taking corrective actions.

The interaction map consists of all risk events reported through quarterly questionnaires.

Relating each reported risk event to another reported risk event determines whether the event is related separately to the business process of a specific organizational unit that reported the risk, or whether such a risk event has an impact on the realization of another risk event that is related to another business process other organizational units in the company. Likewise, whether a risky event by its nature leads to an interruption in the work of business processes of all organizational units and on which the company has no influence, as may be the case when there is an interruption in the supply of electricity or an internet network failure. An example of an interaction map is given in Table 5.

Table 5. The interation map

Interation map	Risk event 1
Risk event 1	-
Risk event 2	X
Risk event 3	X
Risk event 4	X
Risk event 5	X

In this way, it is determined whether there is a risk event that is primary by its character and on which it depends, whether other risk events are only a consequence of its realization, and in this regards the real source is determined that needs to be treated.

The second segment of the risk treatment procedure refers to the preparation of the Risk Register. This document represents a regulatory requirement and contains data related to business processes for which risk analysis has determined which risks have the highest material significance. The essence of the Risk Register consists of the description of the risk, the measured significance, the chosen procedure for treating the risk, the response to the risk in the form of activities and measures taken to mitigate the risk and/or reduce it to an acceptable level, responsible person for execution of the response to the risk, the deadline for the implementation of corrective measures, the date when the verification of the execution of the measure was done, as well as the status of the implementation of the measures, which can be that the measures were executed, in the process of execution, partially executed, or the implementation has not started. In accordance with the regulatory requirements, this control activity is carried out periodically every six months or less if there is a specific need for it [7].

2.3. Risk Communication

Risk communication is the most important feature of the risk management process and it takes place permanently. The exchange of information about risks is transparent and takes place in two directions: from top management to employees and vice versa.

For the understanding the importance of risk management in the company, the Working group for financial management and control periodically submits materials in written or electronic format on topics related to the risk management process. At the sessions of this working group, risk management issues are periodically considered through quarterly questionnaires on realized risk events, risk register, evaluations of internal controls, annual questionnaires on the state of the COSO internal control system, as well as annual reporting on the state of the risk management system [8].

Likewise, an important role in assessing the effectiveness and communicating about risks is played by the internal audit activity established in the company. Internal audit, on its part, and in accordance with its strategies and work plans, conducts engagements of organizational units according to business processes where the materially most significant risks have been identified through risk analysis. These engagements check the effectiveness of the risk management process, internal controls and governing of business process. Through its reports internal audit communicates with the management of the company about the identified risks and ways to manage them in such a way that they are managed within the scale of risk profile and an acceptable risk level. This procedure includes actions related to the creation of a database of recommendations on an annual level, in which the realization of the implementation of given internal audit recommendations is monitored. Implementation of recommendations and removal of identified deficiencies that imply the effectiveness of the system of risk management processes is the scope of work and supervision carried out in this matter by the Audit Committee as a body established in accordance with the regulatory requirements described under the law governing the work of public companies in the country.

In addition to the above, the documentation of the risk management system is an integral part of communication on this issue with regulatory authorities and external controls during their periodic checks. The topic of risk management is an indispensable item in every external control that is carried out, which indicates the importance of the topic for the needs of looking at the way of management and achieving the goals of the company's operations [9].

2.4. Risk Supervision

Supervision of the risk management system is set up to support the application of The Three Lines of Defense Model. This mechanism clearly defines the role and responsibility of management, organizational units, as well as internal audit.

The mechanism itself is designed to ensure the exchange of information on key risks with all interested parties participating in the business risk management process [10].

The first line consists of organizational units of the sectors and they are the holders of the risk management process. This is about organizational units and business processes that are key for performing business activities.

Managers of organizational units and their employees are a resource that manages the business process and who applying procedure activities carries out actions related to the identification and response to risks. In this way, the potential cost and damage that a risk event can produce is directly affected.

Here, the key emphasis is placed on risk awareness as a business principle that indicates the presence of thinking and reacting to the appearance of factors that can lead to the realization of a materially significant risk event.

The second line of defense consists of organizational units that basically support the first line. These organizational units include the departments of commercial and foreign trade affairs, legal, HR, general affairs, financial and accounting affairs, occupational safety and health, and information technology.

Their task is to provide support in the activities carried out by the first line of defense, which relate to the execution of those activities in which the second line also participates, in control activities that ensure the regularity of the execution of process activities of organizational units belonging to the first line of defense.

If this line detects a factor that implies the stated influence of the realization of a risk event, it signals the first line of defense in order to prevent the possibility of the realization of a risk event.

The third line of defense consists of an internal audit activity that considers the effectiveness of risk management from the first two lines of defense and, if they have not identified a risk, it signals how to react to it.

Further transfer of risk supervision is aimed at the work of the Audit Committee as a body that provides support in the work of the Supervisory Board as the highest management body in the company. At its meetings, the Audit Committee considers issues related to the risk management, primarily financial, as well as others that may arise from the performance of the company's activities [11]. In accordance with the informations which are provided by the Internal audit and the Head of the Working group for financial management and control, proposals are made in the form of actions to be taken in order to manage risks effectively.

The ultimate instance consists of the company director and the company's supervisory board. All questions that direct their attention to the topic of risk management are directed at these positions that are at the top of management and business decision-making process in the company. As the holders of the risk management process, by directing them, they provide actions that should be taken in order to manage the company in accordance with the entrusted resources and goals that should be achieved from the company's operations.

3. RISK MANAGEMENT IN PRACTICE - FRAUDULENT ACTIONS

Fraud risk management is an integral part of the Risk Management Strategy and the Financial Management and Control System. For these needs, the Policy of Combating Fraud was defined, based on examples of good risk control practices and fraud response plans. The main objective of the policy is the protection of property and reputation through the adequacy of risk management and the application of controls. The fraud risk management process includes assessing its overall vulnerability to fraud as well as the scope and magnitude of fraud risk from inaccurate financial reporting and misappropriation of assets. The risk is considered periodically or more often if there are negative impacts. A special segment of fraud risk management is the development of fraud awareness, ethical values and employee training.

For the purpose of performing a risk analysis of fraudulent activities, a questionnaire is used that is divided into two key areas in which the potential risk of committing a fraudulent activity is assessed. Those areas are dishonest financial reporting and misappropriation of assets. On the basis of the completed questionnaire, the likelihood of the occurrence of fraudulent actions are considered. When the questionnaire is processed, the analysis of the risk of fraudulent actions is carried out. Risk analysis of dishonest financial reporting and misappropriation of assets is considered in relation to risk factors related to possible incentives/pressures, opportunities and attitudes, i.e. rationalization of fraudulent actions. Each of the mentioned factors is considered in relation to a predefined set of indicators which is considered in relation to risk components, namely impact, likelihood, vulnerability and speed of realization. Each component is assigned one of the offered weights.

Depending on the selected weighting value, a calculated risk value is obtained (impact*likelihood or impact*vulnerability). The value that corresponds to the actual situation is the one that is taken. The evaluation proceeding is carried out according to the principle of self-assessment. Indicators for which it is determined that their measured risk value is at the level of significance that requires risk treatment are taken into consideration with the aim of defining the control measures that should be taken in order to manage the risk of fraudulent actions. The proposed measures are being considered by the Working Group for Financial Management and Control. The established measures are integral part of the Risk Register and as such are binding upon their application at the level of each organizational unit.

On a periodic basis, the execution of measures by organizational units as well as the possibilities for further improvement are considered. A confidential line for reporting fraudulent actions was also created, to which employees can make reports if they have information that may indicate suspicion of fraudulent actions.

According to the Action Plan of the Working Group for Financial Management and Control, employees are trained on topics about the system of ethical values, corruption and fraud.

The Policy of Combating Fraud prescribes the conduct of disciplinary proceedings against employees in order to determine the validity of the suspicion of committing a fraudulent action, as well as to make appropriate conclusions in accordance with the presented argumentation and material evidence.

In connection with the performed procedures, regular reports are carried out, which are an integral part of reporting on the risk management system as well on financial management and control.

3. CONCLUSION

The public company "Nuclear Facilities of Serbia" has successfully implemented the requirements of standards and financial management and control related to the design and implementation of the risk management system. The risk management system is documented, adequate mechanisms have been created for the identification and evaluation of risks, their ranking by importance and the determination of monitoring priorities.

A Risk Register was created, which is periodically reviewed for the effectiveness of the controls applied in order to manage business risks. A system of reporting on the state of the risk management system was implemented. An internal audit activity has been established, which provides assurance services on the effectiveness of the risk management system, internal controls and governing business processes. Likewise, a Working group for financial management and control was formed, which primarily deals with monitoring the risk management system according to the adopted Action Plan for the establishment and further improvement of the financial management and control system.

An Audit Committee was formed to monitor the risk management process and make recommendations for its effective managing. External controls by Certification bodies, External audits and the State Audit Institution gave a positive opinion on the established risk management system in the company.

The risk management process is an integral part of daily activities and as such is integrated into every business process. Further improvement of this system will maintain requirements regarding the introduction of new technologies, business processes and information technologies as support in performing regular business activities.

References

[1] SRPS ISO/IEC 17025:2017, General requirements for the competence of testing laboratories and calibration laboratories;

[2] SRPS ISO 9001:2015, Quality management systems - Requirements;

[3] Law on the Budget System ("Official Gazette of RS", No. 54/2009, 73/2010, 101/2010, 93/2012, 62/2013, 63/2013 - amended, 108/2013, 142/2014, 68/2015 - Dr. Law, 103/2015, 99/2016, 113/2017, 95/2018, 31/2019, 72/2019, 149/2020 and 118/2021);

[4] PUBLIC COMPANY "NUCLEAR FACILITIES OF SERBIA": Risk Management Strategy, Belgrade, Vinča 2018.

[5] PUBLIC COMPANY "NUCLEAR FACILITIES OF SERBIA": Methodology for identifying, measuring, communicating and monitoring risks, Belgrade, Vinča 2018;

[6] SRPS ISO 31000:2019, Risk management - Guidelines;

[7] MINISTRY OF FINANCE, Central Unit for Harmonization: Guidelines for Risk Management, Belgrade, 2020;

[8] Rulebook on common criteria and standards for the establishment, functioning and reporting of the financial management and control system in the public sector ("Official Gazette of RS", No. 89/2019);

[9] PROCEEDINGS OF THE SINGIDUNUM UNIVERSITY INTERNATIONAL SCIENTIFIC CONFERENCE: Risks in modern business conditions, Singidunum University, Belgrade, 2016;

[10] INSTITUTE OF INTERNAL AUDITORS (IIA): Three lines of defense for an effective risk management process and internal control system, Association of Internal Auditors of Serbia, Belgrade, 2013;

[11] Law on Public Companies ("Official Gazette of RS", No. 15/2016 and 88/2019);