DOI:10.17951/h.2018.52.1.201

A N N A L E S
UNIVERSITATIS MARIAE CURIE-SKŁODOWSKA
LUBLIN – POLONIA

VOL. LII, 1 SECTIO H 2018

Lodz University of Technology. Faculty of Management and Production Engineering

ANNA WALASZCZYK

anna.walaszczyk@p.lodz.pl

Risk Management of Processes in the Quality Management System

Zarządzanie ryzykiem procesów w Systemie Zarządzania Jakością

Keywords: risk; management; process; quality; system

Słowa kluczowe: ryzyko; zarządzanie; proces; jakość; system

JEL Code: A120; L230; M110

Introduction

The latest 2015 edition of the international standard laying down the requirements for the quality management system or ISO 9001 that most entrepreneurs are already familiar with is grounded in two types of approaches to management. The process approach being, at the same time, one of the seven principles of quality management[1] is the first of them, whereas the risk-based approach is the other. While the former is rather well-established in the ISO 9001 system, the former, which is concerned with addressing risks in organizational activity, appears not to have featured in the previous editions of the ISO 9000 standards.

This paper aims to achieve two objectives – a theoretical one and a practical one. The theoretical objective is to discuss the process approach and the risk-based

[1] The principles of quality management include: (1) Customer focus, (2) Leadership, (3) Engagement of people, (4) Process approach, (5) Evidence-based decision making, (6) Relationship management, (7) Improvement.

approach as they relate to management as well as to identify interactions and relationships between them. The practical objective consists in a case study of a manufacturing company with regard to the implementation of a risk-based approach in the operation of processes.

1. The process approach in the quality management system

According to the accepted international nomenclature (as given in ISO 9000:2015), a process is a set of interrelated or interacting activities that use process inputs to deliver an intended result that, depending on the context, is called an output, a product or a service. The standards of the ISO 9000 family encourage organizations to use the process approach in the development as well as in the implementation and improvement of the effectiveness of the quality management system in order to achieve greater satisfaction of interested parties. Organizations that want to use the process approach are required to define processes systematically, manage them and their interrelations to achieve the intended results that are compatible with the adopted quality policy and strategic direction of the organization. Processes, as well as the entire system, can be managed with the PDCA cycle (Plan-Do-Check-Act) and a general focus on the risk-based approach. The purpose of this approach is to take optimal advantage of opportunities and prevent potential threats [Norma PN-EN ISO 9001:2015-10P, 2016]. Fig. 1 is a schematic representation of a process and interrelations between its key elements that include inputs preceded by their sources, undertaken activities, process outputs and their subsequent receivers.

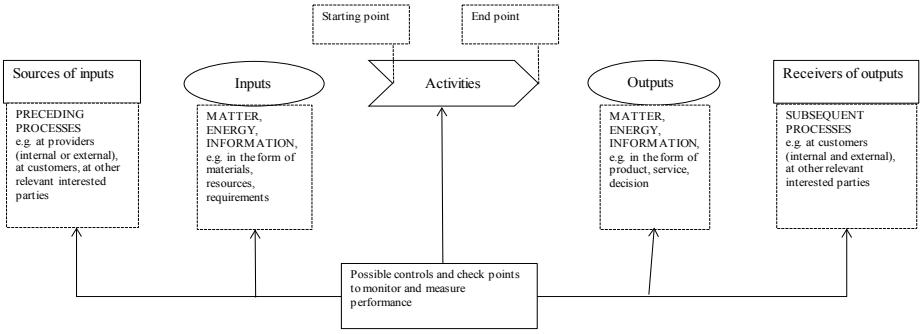

Fig. 1. A schematic representation of a single process

Source: [Norma PN-EN ISO 9001:2015-10P, 2016].

The control and checkpoints for the implementation of monitoring and measurements that are necessary for the control of individual processes become specific to those processes and differ with regard to risks that relate to them.

2. The risk-based approach in the quality management system

Nowadays, the practice of risk management is a necessity for organizations. Properly applied, it increases the resilience of the organization in the face of newly emerging threats. It also facilitates undertaking anticipatory actions, which, in turn, enables optimal use of resources and opportunities for growth [Panasiewicz, 2012].

'Risk' is one of the terms that are common and fundamental in the ISO standards that refer to management systems. It is understood as the effect of uncertainty which may cause a positive or a negative deviation from expectations. Risk is frequently expressed as a combination of the consequences of an event and the associated likelihood of occurrence. The requirements laid down in the PN-EN ISO 9001:2015-10P standard promote understanding of the context of the organization and defining risk as the underpinning of planning. They refer to the necessity of applying risk-based thinking, implementing actions to address risk, and retaining documented information on defining risks. To meet the requirements of this standard, it is crucial that the organization should plan and implement actions to address risks and opportunities, which makes it possible to improve the effectiveness of the quality management system and prevent undesirable effects [Norma PN-EN ISO 9001:2015-10P, 2016].

PN-ISO 31000:2012 is another standard that refers to risk management. The problems of risk management fit into a prominent area of organizational strategic management and are critically significant for rationalization and business continuity [Fałek, 2014]. Processes of risk management should pervade the entire organization. In this regard, it should be analogous to the strategic plan of the organization that is implemented in all areas, levels, and functions in the organization. The developed strategy should ensure that the management of risk enables minimization of losses and development of opportunities to improve management of the organization [Lisiecka, 2012].

To implement the process of risk management, first the organization needs to implement a framework which, according to ISO 31000 (Risk management – Principles and guidelines), includes:

- understanding the organization and its context,
- establishing risk management policy,
- accountability,
- integration into organizational processes,
- resources,
- establishing internal communication and reporting mechanisms,
- establishing external communication and reporting mechanisms.

In the PN-ISO 31000:2012 standard, risk management rests on the three interrelated and complementary pillars (principles, framework, and process). Failing to comply with any one of them results in the organization not being prepared for the objectives of minimizing risk or the occurrence of its potential consequences. These pillars include principles that ensure the effectiveness of the process, a framework

that guarantees the flow of information adequate to the needs, and processes [Wróblewski, 2015, pp. 29–30]. These relationships are presented in Fig. 2.

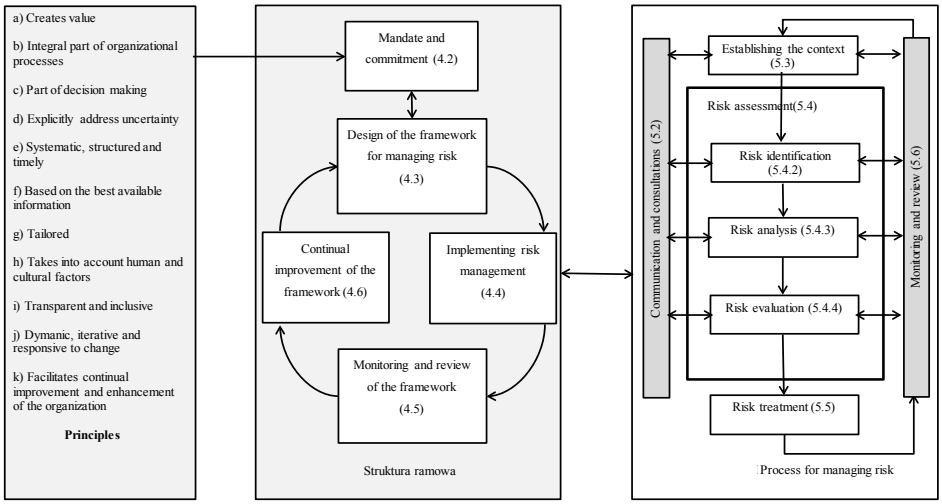

Fig. 2. Relationships between the risk management principles, framework, and process

Source: PN-ISO 31000:2012.

The success of risk management depends on the effectiveness of the management framework providing the foundations, and arrangements that are implemented at all levels of the organization. The PN-ISO 31000:2012 standard requires the organization to include in the design of the framework a strategic analysis of the external and internal context of the organization, and a system of interrelated objectives established by the organization. The analysis of the internal context should include [Urbaniak, 2016]:

- current strategic plan, established objectives, and values of the organization, important success factors e.g. costs, quality, corporate image,
- currently available resources, e.g. personnel, capital,
- current capabilities, e.g. agility, innovativeness,
- organizational structure,
- currently functioning management systems and opportunities for their improvement,
- corporate culture,
- existing information flow system,
- adopted decision making principles and responsibilities of top management.

To ensure the effectiveness of managing risk, it needs to be kept in mind that risk should [Serafin, 2013]:

- create and protect value,

- be an integral part of all organizational processes,
- be part of decision making,
- explicitly address uncertainty,
- be systematic, structured and timely,
- use the best available information,
- be tailored to the context of organizational activity,
- take human and cultural factors into account,
- be transparent and inclusive,
- be dynamic, iterative and responsive to change,
- facilitate continual improvement of the organization.

3. Case study

Enterprise X[2] genuinely operating in the market was the object of the case study. The organization is in the metalworking business. Its main area of activity includes overhauling and modernizing flat-surface, cylindrical, internal, and centerless grinding machines. The services provided by the organization include upgrading grinding machine performance according to client specifications and sale of metalworking machine tools. The core products of the enterprise are used in the automotive and construction industry, and metalworking machine tool manufacturing. The process of design and development occurs at X with regard to the building, remanufacturing and modernizing machines. As for manufacturing of spare parts and machining, the process is carried out based on sketch drawings or templates provided by the customer. To ensure that the customer's expectations are met, the customer is involved in the planning of the design process. The mechanical designer defines the resources and the time required for the completion of the project and determines the final delivery date. Information derived from the design process is presented as technical documentation. All projects carried out by X, depending on their scope and complexity, involve greater or lesser risk. Typically, the risk involved in the projects will be associated with:

- imprecise definition of the scope of the project,
- exceeding the budget allocated for the project,
- delay in the onset of project work,
- poor quality of the provided service.

Apart from potential threats to which services and projects may be exposed to, managing risk also provides opportunities which may have a positive influence on the result. Typical opportunities identified for X's projects include:

- additional work orders from the customer during the performance of the project (change in the scope of work, contract),

[2] Name withheld by request of the organization.

– more effective performance of the project and, as a result, lower costs and/or completion of the project before the deadline.

Identification of opportunities is a constant task during the project performance. Opportunities may be discovered in the process of managing risk because with adequate project management a risk can be transformed into an opportunity. Systematic reviews of managing risks and opportunities in projects enable making decisions to optimize project outcomes. As part of the analysis of X's compliance with the quality management system requirements as set down in PN-EN ISO 9001:2015-10P, a checklist containing 320 questions concerning the requirements was administered. With regard to the process of design, the analysis of the checklist revealed that X takes into account all inputs and all outputs included in the checklist in the process of design and development. However, the problem that the organization has lies in the control of the design process. Mechanical designers, without any control or verification, make decisions on what is right and what is not. Documented information concerning modifications implemented in the process under analysis is not maintained. Lack of adequate management with regard to control of the design process gives rise to a number of threats for the organization. Leaving out the obvious hazards of manufacturing products that do not meet order specifications, and therefore bearing considerable production costs of the product, there is also a major hazard related to the impossibility of proper identification of products which, in turn, interferes with the process of traceability. Thus, if only with regard to the design process, it would certainly be valuable to explore the topic of risk managing in the studied organization.

According to PN-ISO 31000:2012, and PN-EN ISO 9001:2015-10P for the quality management system, the implementation of a risk management system should start with the determination of the context of the organization. To that end, the PEST method (Political, Economic, Social, Technological) may be used which requires that significant factors concerning particular segments of the micro environment be identified, influence of each of the factors on the functioning of the organization and relations between the organization and the micro environment be determined.

The next step involves establishing a risk management policy aligned with the quality policy of the organization. Here, the organization is required to answer the question why it wants to control risk, what its objectives, methods of measuring and reporting risk outcomes will be. One answer to the above question could be for example the desire to maximally minimize risk in the process of production by providing the customer with products that meet requirements in a timely manner.

Next, ISO 31000 requires ensuring accountability associated with risk. The organization under discussion could fulfill this requirement by appointing a team made up of three of its employees with one of them taking the role of the leader who would be responsible for the evaluation of identified risks, recording and reporting their outcomes. The second task would be to assign responsibilities to individual employees for processes with identified risks.

Resources are necessary for managing risk in organizations. With regard to human resources, a three-employee team was appointed and made accountable for managing risk, and individual employees were assigned responsibilities for processes. Each of these employees, if reasonable, should be equipped with a personal computer and other tools depending on their specific needs, e.g. stock controller – access to inventory software, email service, etc. Further, the employees should have access to all forms used in the organization, e.g. a work order form, a material order form. A risk assessment form should be designed for individual processes. It is recommended that employee training in managing risk be given every six months.

Point 4.3.4 of PN-ISO 31000:2012 standard has it that risk management should be embedded in all of the organization's processes. For this to happen, all of the processes should be identified in the organization. These processes could be documented in a process map that includes identification of processes, organization into process groups, and interrelations between these processes. This modification will streamline the process of risk identification and ensure that none of the processes where risk may occur is neglected. The map of processes for the studied organization consists of three groups of processes which include management, core, and auxiliary processes. The core processes form a sequence of planned activities beginning with customer expectations and ending with customer satisfaction.

Once the process map is complete, the next step is to use it in the identification of risks for the processes. It is recommended that a simple form presented in Table 1 (the template gives examples of information that particular fields could be populated with) be developed and implemented. The form helps to create a list of identified risks with assigned responsibilities.

Table 1. Risk identification form

No.	Process	Operation	Threat/Risk	Responsible function
1.	Customer service	....		
2.				
3.				
4.	Design and production planning	....		
5.				
6.				
7.	Purchasing	Procuring raw materials	Incorrect purchase of raw materials and materials	Purchasing specialist
8.		....		
9.				
10.	Taking delivery and storage	Delivery of raw materials	Late delivery	–
11.			Delivered materials fail to meet quality requirements	–
12.			Incorrect materials delivered	–

Source: the author's analysis based on the case study.

Following the identification of threats, an evaluation of risk associated with them needs to be performed. The PHA (Preliminary Hazard Analysis) method is recommended for the company under analysis. The method is rather straightforward as risk is evaluated in terms of the following two criteria:

- S: severity (degree) of potential events,
- P: probability of their potential occurrence.

Once the risk evaluation is completed, the organization will need to monitor acceptable risk but no action will be necessary. However, if the risk is tolerable, appropriate corrective and/or preventive action will need to be taken.

A risk register is created as a result of the risk analysis, which facilitates the rationalization of managing risks. The register could also be created by adding more fields to the repository of risks that would be used for risk evaluation. Risk evaluation for particular processes and control of them by monitoring and implementing appropriate controls will enable effective risk management in the enterprise.

It is recommended that the examined enterprise should perform planned monitoring and risk reviews every six months unless new risks emerge. Should new threats be identified, immediate action would need to be taken. Further, in order to organize all the information concerning risk and its treatment, a risk identification and evaluation manual should be developed for the organization.

In practice at the enterprise under study, during the sale stage, the responsible manager would need to perform a risk analysis of the project that would include the following steps:

- determine an appropriate critical level for each component of the order in terms of cost estimates taking into account, among others, the accuracy of quantity estimates, price per unit,
- input the risk profile into an electronic risk management instrument in order to perform a comprehensive risk evaluation,
- assess all other threats related to the project, consider what mitigation measures might be applied, and determine the net risk exposure (post-mitigation exposure),
- analyze the total risk taking into account the likelihood of contingent risk in order to determine a risk contingency reserve,
- include the final level of risk in the project cost estimate.

The process of determining a risk reserve is presented in Fig. 3.

The process of managing risk as presented in Fig. 3 is mandatory for enterprises for high-value projects. In all other projects, risk is assessed and properly documented at the manager's request and accounted for in the overall project cost estimate. The manager needs to make sure that the risk assessment performed during the stage of the sale and the authority given to him/her to manage risk included in the risk and opportunity management system have been properly accounted for in the project preliminary budget and properly recorded in the electronic project management system.

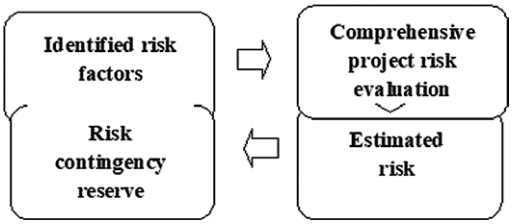

Fig. 3. The process of determining a risk contingency reserve

Source: the author's analysis based on data collected from X.

Conclusions

Risk management can be used by all organizations regardless of their industry and sector. Due to the fact that no unified model of risk management is promoted in the international standards – the model implemented on the basis of the guidelines provided in ISO 31000 is not subject to certification but it nevertheless contributes to the harmonization of and lends support to other standards whose requirements refer to specific types of threats. It was the theoretical objective of this work to demonstrate interrelations between the process approach and the risk-based approach in management. In accord with the literature of the field, the foregoing analysis has revealed the two to be strongly reciprocally dependent because managing risk without relying on a process approach in organizational activity would be extremely difficult if not impossible. To achieve the practical objective of the study, which was the case study of X, a manufacturing enterprise, it has been proven that risk is embedded in the functioning of contemporary enterprises, whereas implementation of the process of managing it becomes increasingly more relevant.

Bibliography

Fałek Z., *Standardy zarządzania ryzykiem jako narzędzia budowania wartości przedsiębiorstw dystrybucji energii elektrycznej*, [w:] Urbanek P. (red.), *Ekonomia i zarządzanie w teorii i praktyce*, t. 2: *Polityka ekonomiczna i zarządzanie przedsiębiorstwem w warunkach kryzysu gospodarczego*, Wydawnictwo Uniwersytetu Łódzkiego, Łódź 2014.

Lisiecka K., *Zarządzanie ryzykiem determinantą jakości zarządzania przedsiębiorstwem*, „Zarządzanie i Finanse" 2012, nr 3, cz. 1.

Norma PN-EN ISO 9001:2015-10P, *Systemy Zarządzania Jakością – Wymagania*, PKN, 2016.

Norma PN ISO 31000:2012, *Zarządzanie ryzykiem – Zasady i wytyczne*, PKN, 2012.

Panasiewicz A., *Metodyka zarządzania ryzykiem zgodna ze standardem ISO 31000*, [w:] T. Borys, P. Rogala (red.), *Orientacja na wyniki we współczesnej gospodarce*, Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu, Wrocław 2012.

Serafin R., *Koncepcja systemu adaptacyjnego zarządzania ryzykiem dostaw w procesach produkcyjnych*, „Zarządzanie Przedsiębiorstwem" 2013, nr 3.

Urbaniak M., *Wykorzystanie koncepcji zarządzania ryzykiem w doskonaleniu systemów jakości*, „Problemy Jakości" 2016, nr 6.
Wróblewski D., *Zarządzanie ryzykiem. Przegląd wybranych metodyk*, Wydawnictwo CNBOP-PIB, Warszawa 2015.

Zarządzanie ryzykiem procesów w Systemie Zarządzania Jakością

Artykuł odnosi się do zagadnień zarządzania ryzykiem. W opracowaniu podano przykład wdrożenia procesu zarządzania ryzykiem w przedsiębiorstwie działającym w środowisku systemu zarządzania jakością ISO 9001. Studium przypadku jest poprzedzone teoretycznym opisem podejścia procesowego i podejścia opartego na ryzyku w kontekście międzynarodowej standaryzacji.

Risk Management of Processes in the Quality Management System

The article refers to the issue of risk management. It gives an example of the implementation of the risk management process in an enterprise operating in an environment of quality management system ISO 9001. The case study is preceded with a theoretical background of the process approach and risk-based approach in the context of international standardization.