MODERN MANAGEMENT REVIEW **2016**
MMR, vol. XXI, 23 (3/2016), pp. 89-96 July-September

Grzegorz OSTASZ[1]
Andrzej PACANA[2]

RISK MANAGEMENT IN ISO 9000:2015 STANDARDS

The paper presents analyses of changes in the revised ISO 9001:2015 on quality management. Additionally a relatively new requirement emerged in the guidelines to a process approach,. It is the need for a systematic approach to risk assessment. In the three-year transitional period, most organizations will implement such an approach to risk assessment. The most difficult to interpret elements of the new standard is an orientation of activities at risk. Orientation of activities at risk is the most difficult elements of the new standard to interpret. Especially, that ISO 9001:2015 does not specify exactly how the implementation of risk management should look like. Therefore, in the article, next to the requirements analysis, the concept of the six-level methods of the approach implementation was proposed. The matrix method was used where two elements were evaluated: probability of risks and potential impact of risks. Each element can be assessed, e.g. in a 6-point scale, assigning different weights. The assessment of the risk probability consists in assigning to each of the risk types the score from 0 to 1 (every 0,2), and the impact assessment on a scale from 1 to 6 (analogous to the notes). When assessing the risk one should remember that the norm, especially in the context of the organization, requires attention not only to the so-called negative risk, but also chances (potential benefits). Both avoidance of adverse events and exploitation of opportunities is the foundation of risk management. The use of the proposed concept can contribute to the efficient and effective implementation of the requirements of ISO 9001:2015.

Keywords: ISO 9001, risk assessment, quality management system, risk management, quality management

1. INTRODUCTION

Environment and economic conditions, which are changing rapidly, make organizations take systematic measures to prevent any inconsistency of internal or external nature. Risk management is becoming an inherent element of management. This aspect of management was heavily exposed in the revised in 2015 ISO 9000 standards on quality management. Of course, previous editions of ISO 9001 also alluded indirectly to the risk of ventures, but they did not do it in such an obvious way as the edition of 2015. Therefore, organizations which have already implemented quality management system, and there are approx. 1.2 million of them in the word, and in Poland approx. 10 110[3], in a transitional period until 15 September 2018 year would have to expose stronger and apply in practice the principles of risk management. Therefore, in the article the analysis of the require-

[1] Prof. dr hab. Grzegorz Ostasz, Katedra Nauk Humanistycznych, Wydział Zarządzania, Politechnika Rzeszowska, al. Powstańców Warszawy 12, 35-959 Rzeszów, e-mail: gost@prz.edu.pl

[2] Dr hab. inż. Andrzej Pacana, prof. PRz, Wydział Budowy Maszyn i Lotnictwa, Katedra Technologii Maszyn i Inżynierii Produkcji, Al. Powstańców Warszawy 8, 35-959 Rzeszów, tel. 17 865 17 55: e-mail: app@prz.edu.pl (Author for correspondence)

[3] *ISO 9001:2015 Aktualizacja*, access: http://www.bsigroup.com/, on 8.09.2016.

ments of ISO 9001:2015 in risk assessment was done. The generalized way of implementing the standard was also proposed. It can be used directly or after modification resulting from the peculiarity of an organization.

2. ISO 9001 – THE REVISION

International ISO 9001 standard is reviewed regularly. The last update was in September 2015. The Technical Committee decided that it was necessary to revise the standard in order to adapt to rapidly changing conditions where organizations were functioning. Among other priorities of the revision the Committee TC 176 decided to implement were:

- supporting organizations in the area of raising customer satisfaction,
- paying more attention to customer needs,
- preparing organizations to function in a more coherent foundation of integrated management systems,
- paying closer attention to the environment in which organizations operate,
- ensuring that the new standard meets the needs of all stakeholders,
- drawing attention to the need to continuously analyze risks and opportunities[4].

The prepared draft of ISO 9001:2015 standard was distributed for an evaluation and reviews already in 2014. The Committee gathered about 3,000 comments, which were later included in the final version of the standard.

The new (from 2015) standard was drawn up in an innovative form (ISO REGULATION – ANNEX SL 2013), which is common for all new standards of management systems. This should allow an easy integration of systems in the implementation of more than one system[5]. The already mentioned annex imposes a common text, a common structure and terminology in all of the revised standards: ISO 9001, ISO 14001, OHSAS 18001 (ISO 45000) and ISO 27001[6]. The current table of contents of ISO 9001 is as follows:

1. The scope.
2. Normative reference.
3. Terms and definitions.
4. Context of the organization.
5. Leadership.
6. Planning.
7. Support.
8. Operational activities.
9. Evaluation of the effects.
10. Improvement.

Annex A (informative) Explanation of the new structure, terminology and concepts. Annex B (informative) Other International Standards on quality management and quality management systems developed by ISO / TC 176.

---

[4] *Znaczenie ryzyka w zarządzaniu jakością. Jak podchodzić do zmian?, access*, *http://www.bsigroup.com/ISO-9001-2015,* on 8.09.2016.

[5] L. Jodkowski, *Possibilities and Methods of Risk Assessment under ISO 9001: 2015,* IJMSR, 2015, Vol. 3, Is. 10, pp. 14–23

[6] A. Kleniewski, *Zarządzanie ryzykiem w systemach zarządzania jakością, środowiskiem, bezpieczeństwem i higieną pracy – praktyczne rozwiązania,* „Problemy Jakości", nr 11, 2011, R. 43, pp. 23–27.

Bibliography[7].

In line with the priorities in ISO 9001:2015 the main proposed changes are:

- requiring the use of a process approach,
- focus on leadership,
- paying attention to risk management,
- emphasis on goals, measurement and change management,
- communication and awareness,
- lower number of requirements as orders[8].

Looking more specifically looking at the changes in ISO 9001:2015 one may notice that:

- the information on the approach system was removed,
- requirements for cooperation with suppliers were replaced by "relationship management",
- the requirements concerning quality manual were removed,
- preventive actions were abandoned,
- information concerning process management, which have not constituted requirements so far, after the revision became requirements – the rank of process increased,
- thanks to procedures the system became less bureaucratic (with the exception of the required system procedures),
- requirements concerning risk management appeared.

The standard introduces a set of requirements, which, as it is planned, will remain valid for at least the next ten years or longer. The requirements are rather general, but are associated with modern management. The requirements apply to all types and sizes companies, regardless of the sector of the economy. Focusing on the effective management of processes, the standard requires at the same time to pay attention to the risk that accompanies any activity. The compliance with these requirements seems to be the key to competitive success of many organizations.

3. RISK MANAGEMENT IN ISO 9001:2015

One of the major changes in the updated ISO 9001:2015 is a systemic approach to risk. The standard makes manage risk in a systematic way, rather than treating it as a single element of the quality management system as it was before. In previous editions of ISO 900 the risk appeared in the section on preventive measures, which in current edition has been removed. Assuming the current approach based on risk assessment, the organization consciously and actively should prevent or reduce side effects by promoting a continuous improvement[9].

ISO 9001:2015 standard in its requirements did not specify the methodology or does not make adhere to specific standards in the area of risk, i.e. e.g.:

- PN-ISO 31000:2012 Risk Management – Principles and guidelines,

[7] *PN-EN ISO 9001:2015-10 – Polish version*, PKN, Warszawa 2016.

[8] *PN-EN ISO 9000:2015-10 – Polish version*, PKN, Warszawa 2016.

[9] S. Zapłata, *Methods of Risk Assessment for the Purpose of Normalized Management Systems Implementation*, "Współczesne Zarządzanie" 1/2012, pp. 9–19.

- ISO 22301 Business continuity management system,
- ISO 19600 Compliance of management systems – Guidelines,
- Standard risk management FARM 2002 – Directives of the organization Federation of European Risk Management Associations,
- Management of corporate risk – integrated framework structure, COSO 2004.

The standard puts a great emphasis on taking into account the requirements for understanding, "the organization and its context" and "needs and expectations of stakeholders". On this basis, it is necessary to manage skilfully the specific risks which are adapted to the specific organizations. It follows that for all types of organizations there is a need to understand the risks undertaken by the pursuit of goals[10]. Above all, organizations must understand the overall level of risk in their processes and operations. Risk processes affect the measurement results and processes which in turn are correlated with the objectives of the system stored in the policy of quality. Thus, the risk of uncertainty concerns the implementation of the objectives of the scheme, which is to provide products according to customer requirements. Knowing the risks and discovering ways in which risks can be mitigated, the organization gets an opportunity to make changes for the better or could improve. The requirements for risk management are presented in Table 1.

Table 1. Generalized requirements of ISO 9001:2015 in terms of risk-based approach

In Point 4 organization is required to identify threats that may affect its ability to achieve the objectives of the system. It is recognized that the consequences of the risks are not the same for all organizations.	In Point 5 management is required to demonstrate leadership and to ensure that the risks and opportunities that may affect compliance with the requirements for the product or service, are defined and allocated.
In Point 6 the standard requires that the organization is required to identify risks and plan a way to address the identified threats and chances.	In point 7 the standard requires the establishment of risk management processes.
In Point 8 the requirements are: monitoring, evaluation, analysis and verification of risk and the possibility of a chance.	In Point 9 the organization is committed to measure and evaluate risks and opportunities.
In Point 10 the organization is committed to excellence by responding to changes in risk.	

Source: own research based upon[11].

Speaking about the risks it should be emphasized that the norm, especially in the context of the organization requires attention not only to the so-called negative risk, but also the chances (potential benefits). Both the avoidance of adverse events as well as the exploitation of opportunities is the foundation of risk management.

[10] *PN-ISO 31000:2012, Zarządzanie ryzykiem – Zasady i wytyczne,* PKN, Warszawa 2012.

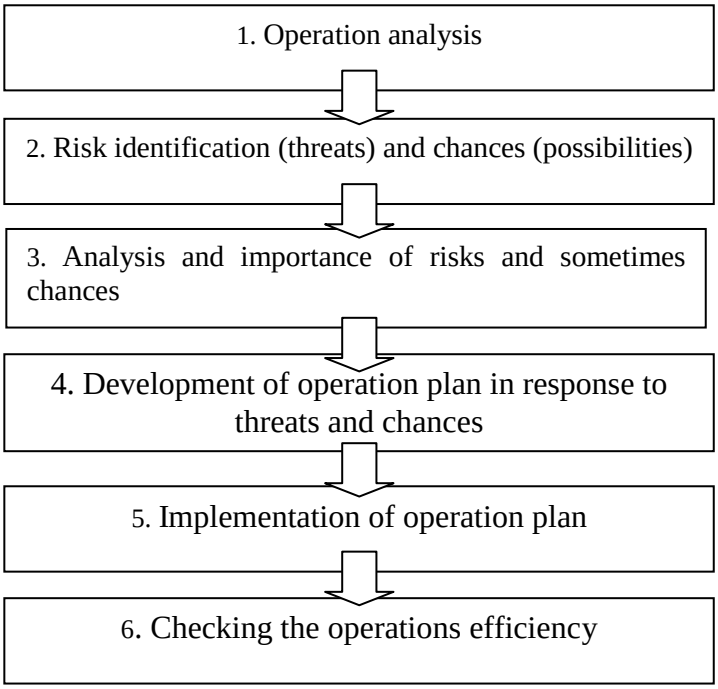
[11] *PN-EN ISO 9001:2015-10 – Polish version,* PKN, Warszawa 2016.

4. AN APPROACH DIRECTED TO RISK ASSESSMENT

Orientation of activities at risk is one of the most difficult elements of the new standard to interpret. Especially, that ISO 9001: 2015 does not specify exactly how the way of implementation of risk management should look like.

The introduction of the requirements of ISO 9001:2015 in some organizations in terms of risk management will not change or changes are very little. The vast majority of organizations will only have to implement a targeted approach to risk assessment in their organizational processes. Methodically it can be done in 6 steps as shown in Fig. 1

Fig. 1. Methodology of the approach based upon the risk



Source: own research based upon[12].

Based on the analysis of mostly current business activity and identified processes, one should adopt a method of identifying risks. Most often in organizations that have implemented environmental management systems or safety standards such activities do not cause a problem, because they are performed routinely.

Identification of risk as the most important part of risk management is not limited to the area of threats, but also to seek opportunities. It is based on a detailed analysis of the various situations that may cause a positive or negative impact on the safety of patients and the interruption or disruption of the continuity of the organization.

[12] *PN-ISO 31000:2012 Zarządzanie ryzykiem – Zasady i wytyczne...*

In the risk identification two distinct phases can be distinguished: an initial or continuous identification. Risk should be sought within and outside the organization.

There are many tools that can be used for risk identification, e.g.: brainstorming, check lists, scenario analysis, FTA or HACCP.

Each risk should have its owner (as in process management), who is responsible for ensuring that it is managed and monitored.

An analysis and the importance of risks is a stage based on two documents: the risk register and risk map. Previously the method of assessment of previously identified risks should be adopted. For the risk assessment the matrix method should be used, within which there are evaluated two elements:

- the likelihood of risks and
- the potential impact of risks.

Each element can be assessed, e.g. in a 6-point scale, with assigning different weights. For instance, the assessment of the likelihood of the risk consists in assigning to each of the types of risk the score from 0 to 1 (0,2), and the impact assessment on a scale from 1 to 6 (analogous to the notes at school). The examples of such tables are presented in table 2 and 3.

Table 2. An exemplary, generalized table of probability of risk selection

Points	Name	Results description
0	Minimum	The risk does not exist / can occur in quite exceptional circumstances.
0,2	Low	The risk probably will not occur. Over the last year the area / process was not subject to organizational changes The process is governed by a small number of internal and external regulations
0,4	Medium	There is a probability of risk in the next 3 years. Over the last year the area / process was subject to small organizational changes. The process is governed by a small number of internal and external regulations.
0,6	High	There is a high probability of risk in the next 2 years. Over the last year the area / subject to the process of organizational changes.
0,8	Certain	The risk will occur within the next year. The threats are related to tasks within the strategic objectives. The process is regulated by a large number of internal and external regulations.
1,0	Critical	The risk will take place several times over the next year. Threats are related to tasks within the strategic objectives. The process is regulated by a large number of internal and external regulations.

Source: own research.

Table 3. An exemplary, generalized table of potential outcomes selection

Points	Name	Results description
1	Minimum	Possible effects are mitigated by existing control mechanisms
2	Small	Existing control mechanisms should reduce the impact of potential disturbances
3	Medium	Existing control mechanisms to some extent can reduce the impact of potential disturbances
4	Relevant	Existing control mechanisms only to a small degree can reduce the impact of potential disturbances
4	Serious	Low effectiveness of existing control mechanisms
5	Disastrous	The lack of appropriate control mechanisms or existing mechanisms are ineffective – serious disturbance in the work of the unit; threats will make the lack of continuity

Source: own research.

The accepted risk map can be in the form of a results matrix and the likelihood of occurrence. It attributes the values to individual fields (the product of the probability and effect) and with the colour or the description establishes insignificant, moderate and significant risk values. The register should be created on the basis of adopted risk maps in the organization. It describes the risks identified in the operational areas related to the functioning of the organization. The team for risk management then hierarchizes the risks.

The tools for analysis and risk assessment can be e.g.: scenario analysis, decision tree or FMEA.

The result of work related to the analysis and evaluation of risk is the ranking according to significance criteria, which directly leads to the development of action plans, their implementation and effectiveness control. These activities are highly dependent on the specifics of the organization and identified threats.

5. CONCLUSIONS

The revised ISO 900 standard introduced also the requirements related to the process approach and risk management. This fact will soon force onto many organizations the need for an approach based on risk assessment. Organizations that have not yet done it may support themselves with the methodology which allows meeting the requirements of ISO 9001:2015. An additional benefit of a successful risk management will be probably following the commands, safety, and an improvement of the decision-making process. It is worth noting that the risk-based approach is not new. Often such actions were performed, but it was not necessarily a systemic and continuous operation. Now this is required by a new standard, and this requirement is dictated by the desire to put the organization on the path of smoother and more efficient management.

REFERENCES

[1] *ISO 9001:2015 Aktualizacja*, access: http://www.bsigroup.com/, on 8.09.2016.
[2] Jodkowski L., *Possibilities and Methods of Risk Assessment under ISO 9001: 2015*, "International Journal of Managerial Studies and Research (IJMSR)", Vol. 3, Issue 10, October 2015, pp.14–23.
[3] Kleniewski, A., *Zarządzanie ryzykiem w systemach zarządzania jakością, środowiskiem,*

bezpieczeństwem i higieną pracy – praktyczne rozwiązania, „Problemy Jakości" nr 11, 2011, R. 43, pp. 23–27.
[4] *PN-EN ISO 9000:2015-10 – Polish version*, PKN, Warszawa 2016.
[5] *PN-EN ISO 9001:2015-10 – Polish version*, PKN, Warszawa 2016.
[6] PN-ISO 31000:2012 *Zarządzanie ryzykiem – Zasady i wytyczne*, PKN, Warszawa 2012.
[7] Sęp, J., Perłowski, R., Pacana, A., *Techniki wspomagania zarządzania jakością*, Oficyna Wydawnicza Politechniki Rzeszowskiej, Rzeszów 2016.
[8] Zapłata S., *Methods of Risk Assessment for the Purpose of Normalized Management Systems Implementation*, "Współczesne Zarządzanie" 1/2012, pp. 9–19.
[9] *Znaczenie ryzyka w zarządzaniu jakością. Jak podchodzić do zmian?,* access: http://www.bsigroup.com/ISO-9001-2015, on 8.09.2016.

ZARZĄDZANIE RYZYKIEM W STANDARDACH NORMY ISO 9000:2015

W opracowaniu zaprezentowano wyniki analizy zmian, jakie niesie znowelizowana norma ISO 9001:2015 dotycząca systemowego zarządzania jakością. Obok wymagania stosowania podejścia procesowego, pojawiło się stosunkowo nowe wymaganie. Jest nim konieczność systemowego podejścia do oceny ryzyka. W trzyletnim okresie przejściowym większość organizacji będzie musiała takie podejście do oceny ryzyka wdrożyć. Zorientowanie działalności na ryzyko stanowi jeden z trudniejszych do interpretacji elementów nowej normy, zwłaszcza że ISO 9001:2015 nie precyzuje dokładnie, jak ma wyglądać sposób wdrożenia zarządzania ryzykiem. Dlatego też w opracowaniu obok analizy wymagań zaprezentowano koncepcję sześciostopniowej metodyki wdrożenia podejścia opartego o ocenę ryzyka. Do oceny ryzyka wykorzystano metodę macierzową, w ramach, której oceniane były dwa elementy: prawdopodobieństwo wystąpienia ryzyka i potencjalne skutki wystąpienia ryzyka. Każdy z elementów zaproponowano ocenić w 6-stopniowej skali i z przypisaniem różnych wag. Ocena prawdopodobieństwa wystąpienia danego ryzyka polegać ma na przypisaniu każdemu z rodzajów ryzyka punktacji od 0 do 1 (co 0,2), a ocena skutków w skali od 1do 6 (analogicznie do ocen). Oceniając ryzyko należy pamiętać, że norma, szczególnie w kontekście organizacji, nakazuje zwrócenie uwagi nie tylko na te tzw. negatywne ryzyka, ale również na szanse (potencjalne korzyści). Zarówno unikanie niekorzystnych zdarzeń, jak również wykorzystywanie szans jest fundamentem zarządzania ryzykiem. Zastosowanie zaproponowanej koncepcji może się przyczynić do sprawniejszego i efektywniejszego wdrożenia wymagań ISO 9001:2015.

Słowa kluczowe: ISO 9001, ocena ryzyka, system zarządzania jakością, zarządzanie ryzykiem, zarządzanie jakością

DOI: 10.7862/rz.2016.mmr.29

Tekst złożono w redakcji: kwiecień 2016
Przyjęto do druku: sierpień 2016