

THE ROLE OF RISK MANAGEMENT IN ISO 9001: 2015

Cătălina Soriana SITNIKOV¹
Claudiu George BOCEAN²

ABSTRACT

Organization's quality management system will experience substantial changes when the final draft of ISO 9001: 2015 will be published and will become operational. Therefore, organizations must be informed in advance about the changes that are anticipated to be ready to implement the revised requirements of the standard. An important direction given by new version of the standard consists in a growing emphasis on managing risks faced by the organization and valorisation of the opportunities that may arise. In the present paper we conducted a review of the main changes to the ISO 9001: 2015 and a critical analysis regarding risk management approach in the new version of the standard. Given that ISO 9001, as amended and published this year, will move to a new stage in the structure and objectives oriented towards risk management and identifying and implementing opportunities, continuous improvement, the most important component of quality management must be seen from risk perspective. Thus, based on exploratory research the authors designed and developed a tool (an integrated risk management model) that could streamline the process of continuous quality improvement. In authors' opinion, it would be desirable a more detailed and applied approach to risk management and quality continuous improvement correlation in the new standard.

KEYWORDS: *ISO 9001:2008, ISO 9001:2015, risk management, risk-based thinking, risk tolerance, PDCA*

JEL CLASSIFICATION: *L15*

1. INTRODUCTION

The efficiency and profit maximization are the core objectives of any organization. Regardless of size, sector or geographical location, all companies are constantly looking to maximize their profits. ISO 9001 was designed as a standard for organizations seeking to optimize their operational excellence, being increasingly important as end users want increasingly more to get high quality products (TUV SUD, 2014). First published in 1987, ISO 9000 has consistently been the most popular series of ISO standards. Standards ISO 9000 formed a basis for developing other management systems, including environmental, occupational health and safety, information security, energy, etc. Standard "ISO 9001: 2008 Quality Management Systems - Requirements" is widely used in many industries such as aerospace, telecommunications, education, health and government bodies. Taking as a basis the results of this standard for the last 25 years, ISO shall ensure that the standard will continue to provide a solid foundation for quality management in the next 25 years. In a survey conducted among users ISO Committee responsible for ISO 9001 decided that it is necessary to review the following directions (BSI, 2014): integration with other management systems, providing an integrated approach to organizational management, providing a

¹ University of Craiova, Romania, inasitnikov@yahoo.com.

² University of Craiova, Romania, boceanclaudiu@yahoo.com.

consistent basis for the next 10 years, capturing the more complex organizational contexts, reflecting the needs of all potential users, enhancing an organization's ability to meet its customers. Through the changes they expected both in structure and in content, ISO wants the ISO 9001:2015 to have the widest possible range of application, not just in enterprises producing goods but also in enterprises from services sector. The services sector has exceeded substantially the producing goods sector, therefore it needed a standard that covers all aspects of production, including production services. ISO 9001:2015 will lead, in this respect, to a significant improvement, to a strategic integration of the providing products and services processes in the center of organization's activity (NQA, 2015). Winters (2014) believes that in ISO 9001:2015 a major focus is placed on gaining added value to the organization and its customers.

For any organization, the degree of modification of processes, procedures, documents will depend on the maturity and effectiveness of current management system, organizational structure and practices from quality management area. NQA (2015) recommends that the organization to carry out an analysis in order to highlight the differences between the two versions of ISO 9001 to identify financial, human and time resources necessary for the transition to the new version.

In this paper we made a brief overview of the main changes in the new version of ISO 9001, insisting on risk management area, because ISO 9001, as amended and published in September 2015, moves to a new stage in the structure and objectives oriented towards risk management and identifying and implementing opportunities. In these conditions, continuous improvement and procedural approach will be maintained, but seen and approached from a new perspective, risk management generating opportunities or "positive uncertainty" (Bureau Veritas, 2015).

Following a critical analysis of the new version of the standard and literature we have shown that the new version although it introduced the concepts of risk and risk-based thinking could be improved by a more detailed and applied approach. In this paper, based on an exploratory research undertaken it was proposed the use of an instrument we developed by integrating the two methodologies (risk management and PDCA) that could streamline the process of continuous quality improvement. Implementation of the proposed new instrument would meet the needs of all stakeholders of the organization in conditions of maximum profitability.

2. LITERATURE REVIEW

The main changes that are anticipated by ISO refer to both the structure and the content and essence of ISO 9001: 2015. The most relevant changes in the standard are reviewed by Rapaport (2014): increase main clauses from seven (ISO 9001:2008) to ten (ISO 9001:2015), paying special attention to risk management, focus on organization and customer value, paying special attention to the organizational context in achieving excellence in quality control changes to requirements documents, paying special attention to leadership.

The structure including now 10 main clauses is mainly aimed to facilitate the possibility of harmonization and integration of ISO 9001: 2015 with other standards to enable multiple certifications without problems faced by organizations today (Perry Johnson Registrars, 2015).

Since ISO 9001:2008 uses the generic term product to define products, services, processes and hardware were observed difficulties among businesses that do not belong to the production of material goods regarding the application of this standard (Hunt, 2014). Given that the service sector exceeded 70% of total production in developed countries, it is necessary to have a standard that is clearly aimed at this area. Therefore the phrase "product" was replaced with "goods and services" when referring to what is delivered to customers. The term "services" is used separately to highlight the differences between products and services in the application of some requirements of the standard, but in most cases, the terms are used together. There is a possibility that in some cases the term "product" being used separately only to specify that a certain requirement is specific only to products.

Regarding quality control document management, standard ISO 9001: 2015 introduces flexibility in the process, passing to a holistic view that takes into account the integration of technology in both the basic processes of production, and especially the support processes.

This opportunity will allow an organization to certify several standards at the same time, the option for one or more standards being guided by economic sector (Winters, 2014). Compared to the previous version it added the context of the organization that in his opinion of Hutchins (2014) involves a broader way of building quality management system.

Tseros (2015) considers that the main benefits brought by the new version of ISO 9001: 2015 are:

- ensuring compatibility with other standards;
- reducing duplication and conflicts that arise between different standards of a management system;
- minimizing the necessary documentation.

Hunt (2014) believes that the revised standard will focus on application requirements and not on exceptions to these requirements. There are no defined boundaries outside which clauses may lose applicability. The justification will be needed just to illustrate that a limited application of a clause does not affect the organization's ability to supply products and services (Hunt, 2014).

The main changes in terminology that occurred in the new version of ISO 9001 (currently yet in the proposal stage) are presented in Table 1.

Table 1. Terminology changes

| ISO 9001:2008 | ISO 9001:2015 |
|--------------------|--|
| Products | Products and services |
| Exclusions | Application Documented Information |
| Documents, Records | Environment for the operation of processes |
| Work Environment | Environment for the operation of processes |
| Purchased Product | Externally provided products and services |
| Supplier | External Provider |

Source: Hunt, 2014

If ISO 9001: 2000 and ISO 9001: 2008 were based on the process approach, the new version of ISO 9001: 2015 has an approach based mainly on requirements. Process approach is maintained including new requirements in addition to previous versions: expected inputs and results, determination of risks and opportunities, determination of the performance indicators necessary to demonstrate that the processes are effective, assigning responsibilities and authorities, changing processes to get expected results.

Risk management is now an important aspect of any quality management system. ISO 9001: 2015 recognizes in its preamble the importance of "risk-based thinking" and considers risk management must now extend to "external delivering of goods and services" and should not target only core processes. Deysher (2015) opines that ISO 9001 included, by default, the concept of risk management, therefore the 2015 version of the standard is more explicit and incorporating this concept into the management system.

Risk-based thinking, already part of the process-based approach makes, in the new version of the standard, from preventive action an integral part of the process. Although risk-based thinking has as main objective the prevention of risks, thereby through it can also identify and seize opportunities (positive risks). Although risk management is integrated into the management system the proposal for revision not much details actions that should be taken. It specifies that organizations seeking a

more complex risk management may use ISO 31000 which provides guidance on the management of risks which may be appropriate in some organizational contexts. However in the ISO 9001:2015 there is no requirement to do so.

3. RISK MANAGEMENT APPROACH IN ISO 9001: 2015

One of the purposes of a quality management system is a tool for risk prevention (Hunt, 2014). In the proposal for ISO 9001:2015 there is no separate clause addressing risks. The concept of risk prevention actions is defined in the introduction (0.5 "Risk-based thinking") and the main clause six (Planning for the quality management system), namely in clause 6.1 (Actions to address risks and opportunities). This clause provided the risks and opportunities to be addressed in the planning of the quality management system (ISO 2015): ensuring that the quality management system can achieve planned results, prevent or reduce the undesirable effects of emerging risks, obtaining continuous improvement.

Organization will plan actions needed to address these risks and opportunities and ways of implementing the actions in quality management system processes. Actions taken to address the risks and opportunities are proportionate to the potential impact on the products and services.

ISO 9001: 2015 considers that not all the quality management system processes represent the same level of risk in terms of its capacity to meet the objectives and the consequences of non-compliance processes, products, services or systems are not the same for all organizations (ISO, 2015). For some organizations, the consequences of non-conforming requirements of products and services can only result in minor inconvenience for the customer. For other organizations, the consequences may be higher and may have significance and impact. "Risk-based thinking" as defined in ISO 9001: 2015 allows choosing the degree of planning and control quality management system and its component processes and activities.

In practical terms "risk-based thinking" is based on the concept of risk tolerance level. Risk tolerance is the ability of an organization to accept or avoid risk. Organizations that are willing to accept a high dose of risk are called speculator organizations, while that the organizations avoiding the risks are called conservative organizations.

An example of the acceptability of risk degree is illustrated in Figure 1, in an axis system with two variables: the probability and risk impact.

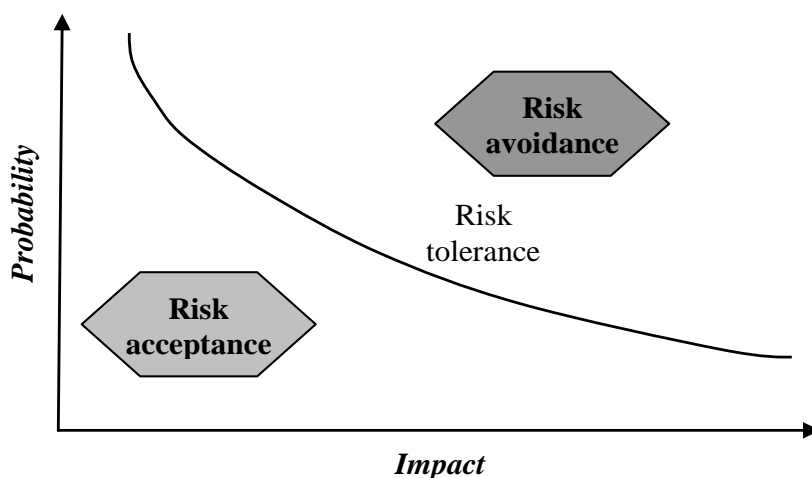


Figure 1. The degree of risk acceptability

Source: developed by authors

Acceptable risks are those placed below the risk tolerance curve, while unacceptable risks are placed above the curve. Curve position within the axis system is determined by the degree of

acceptance of risk to an organization. The two categories of organizations (speculator and conservative) are shown in Figure 2.

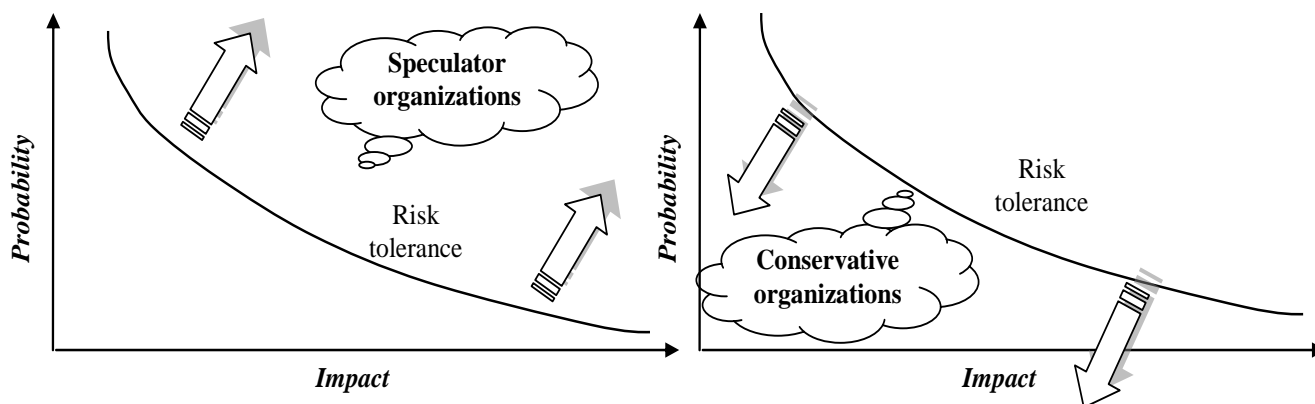


Figure 2. Trends of speculator and conservative organizations in managing risks

Source: developed by authors

While speculator organizations assume greater risks than the acceptable average (tolerance curve moving towards the top right of the graph), conservative organizations avoid possible risks (translating tolerance curve towards the bottom left of the graph). However, most organizations define their risk tolerance in a range located between the two extremes.

In our opinion insufficient risk management approach in ISO 9001:2015 may be satisfactory for speculator organizations. Also conservative organizations ISO 9001: 2015 make recommendation to use ISO 31000. The vast majority of organizations with a moderate tolerance for risk remain uncovered in ensuring the effective management of risk.

Therefore we believe that it would be desirable that a clause of ISO 9001: 2015 to target the entire risk management process without reaching too high a degree of detail, following that the ISO 31000 to come in addition for those organizations who wish to develop further this process. In our opinion, risk management process which could have included a specific clause should suppose five stages (Figure 3):

- planning of analysis activities which is divided into three sub-phases (addressing, planning and execution of the activities);
- risk identification is the stage where they are established risks and their characteristics;
- quantifying risks include subsequent two components (qualitative analysis - prioritizing risks according to their impact and probability of occurrence, quantitative analysis - quantitative determination of the effects of risks materializing on the organization's objectives);
- reaction to the materialization of risks (alternative development for the materialization of risks);
- monitoring and control of risks involves activities such as tracking of identified hazards; monitoring residual risks; identification of emerging risks; execution of the risk response plan; assessing the effectiveness of reactions).

Moreover, these phases of risk management should be integrated to methodology known as "Plan-Do-Check-Act" (PDCA) under the ISO 9001: 2015. This instrument, that we proposed, obtained by integrating the two methodologies would be more effective in the process of continuous quality improvement and can be applied in all processes as well as in the quality management system as a whole.

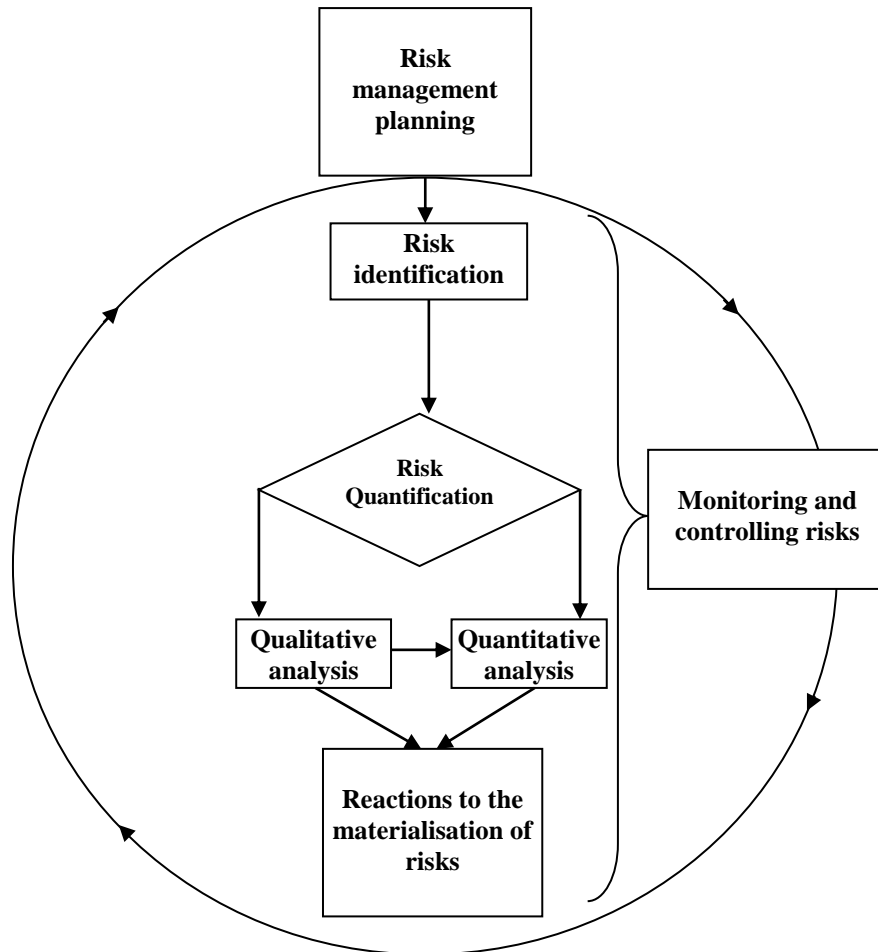


Figure 3 Risk management process
 Source: developed by authors

The ways of integration which we consider to be viable is shown in Figure 4.

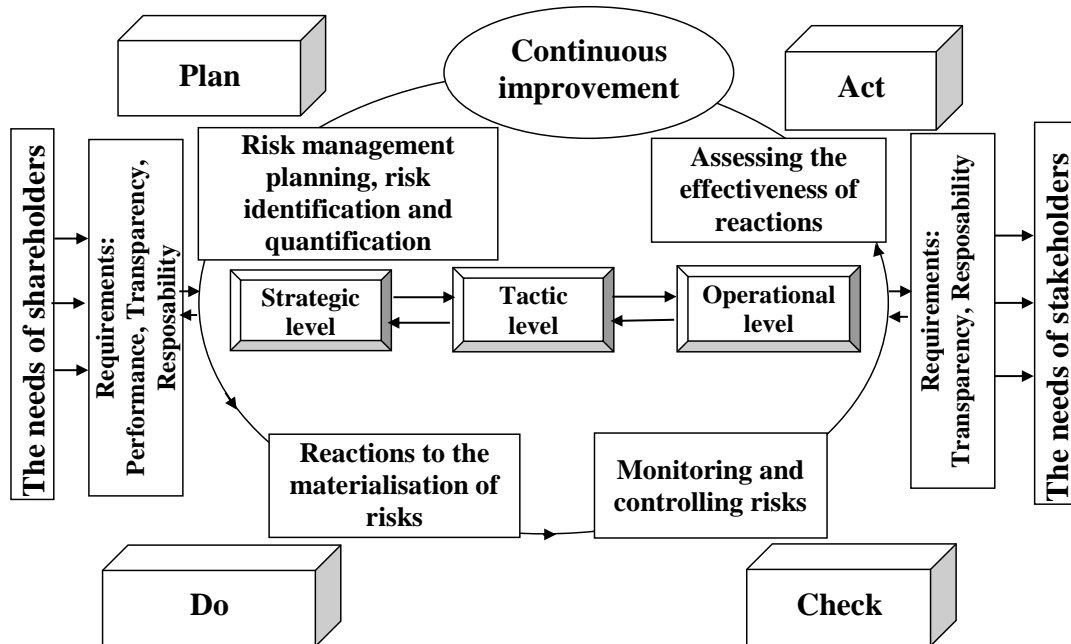


Figure 4 Integrating PDCA with risk management stages
 Source: developed by authors

The model developed by us is designed to operate at all three levels of implementation: strategic (long-term, under the responsibility of top management), tactical (medium term, under the responsibility of each department), operational (short term, under the responsibility of teams work and individuals).

4. CONCLUSIONS

To cope with the changes imposed by the new version of ISO 9001 organizations must prepare to adapt quality management system to meet the new requirements and transitional terms. The main objectives of ISO 9001 have been and still providing increased confidence in the ability of the organization to consistently provide products and services and increase customer satisfaction. Uncertainty about achieving these goals has led to the explicit introduction of the concept of "risk" and the syntagma "risk-based thinking" in vision of ISO 9001:2015. The concept of risk was included in ISO 9001 from the beginning but has not been explicitly formulated. Risk-based thinking, defined by ISO 9001: 2015 is a type of thinking that any individual does automatically, most often unconsciously. Following this new revision, ISO substantiates whole quality management system on this thinking.

However, in our opinion ISO sweeps between two levels of risk, ignoring the average level. If for speculator organizations with a high tolerance for risk, new risk management requirements set out in ISO 9001: 2015 are sufficient and for conservative organizations with a low tolerance for risk is recommended ISO 31000, organizations with average level of risk tolerance remain outside the scope of standardization. They can use ISO 31000 requirements, but financial and human resources involved would lead to increased costs. In our opinion it would be necessary to introduce a clause to explicitly include the risk management and / or creating a tool by integrating the stages of PDCA with steps of risk management. This tool that we propose in this paper can help organizations to continuously improve their quality processes, activities, products and services by preventing and combating risks and seize opportunities.

REFERENCES

- BSI. (2014). ISO 9001 Whitepaper - Understanding the changes. Retrieved May 27, 2015 from: <http://www.bsigroup.com/LocalFiles/en-IN/Resources/ISO%209001/ISO-9001-Whitepaper-Risk-in-quality-management.pdf>
- Bureau Veritas. (2015). ISO 9001:2015 – What are the main changes?, Retrieved August 14, 2015, from <http://www.revision2015.com/iso-90012015-what-are-the-main-changes/>
- Deysher, B. (2015). *A Risk Based Thinking Model for ISO 9001:2015*. Retrieved September 24, 2015 from: <http://rube.asq.org/audit/2015/01/a-risk-based-thinking-model-for-iso-9001-2015.pdf>
- Hunt, L. (2014). *ISO 9001:2015 - Understanding the Key Changes*. Lorri Hunt & Associates Inc. 2014. Retrieved May 18, 2015 from: <http://foro-internacional-de-la-calidad.icontec.org/memorias/CONFERENCIAS/JUEVES%20AGTO%2028/17.%20%20JV%20-%20ACTUALIZACION%20ISO%209001%20-%20LORRI%20JUNT-3.pdf>
- Hutchins, G. (2014). *Risk management & ISO 9001:2015*. Retrieved September 26, 2015 from: <http://insights.ceracademy.com/files/2014/04/AmCon-Presentation1.pdf>
- IAF. (2015). *Transition Planning Guidance for ISO 9001:2015*. International Accreditation Forum, Inc. IAF ID 9:2015, Issue 1. Retrieved May 18, 2015 from: <http://www.iaf.nu/upFiles/IAFID9Transition9001PublicationVersion.pdf>
- ISO. (2008). *ISO 9001:2008 Quality management systems - Requirements*.

- ISO. (2015). *ISO 9001:2015 Quality management systems - Requirements*.
- NQA. (2015). *ISO 9001:2015 Transition gap analysis*. Retrieved May 24, 2015, from <https://www.nqa.com/Nqa.com/media/PDF-Download-Documents/NQA-ISO-9001-2015-Gap-Analysis-Documents.pdf>
- Perry Johnson Registrars, Inc (2015). *Preparing for the Change – Transition to ISO 9001:2015*. Retrieved September 25, 2015 from: <http://www.pjr.com/downloads/ISO%209001%20Transition%20FAQ.pdf>
- Rapaport, M. (2014). Big Changes Anticipated for ISO 9001: 2015. Retrieved May 18, 2015, from <http://www.iqs.com/iqs-blog/big-changes-anticipated-iso-9001-2015/#comment-855>
- TUV SUD. (2015). Navigating ISO 9001:2015 Understanding why the new ISO 9001 revision matters to everyone. White paper. Retrieved May 21, 2015 from: <http://www.tuv-sud.com/uploads/images/1415334301540598481613/tuv-sud-navigating-iso-9001-2015.pdf>
- Tseros H. (2015). *The new ISO 9001:2015 Standard. Overview of Changes*. Retrieved September 25, 2015 from: <https://www.wmo.int/aemp/sites/default/files/WMO-TT-QMF-4-AI12-FromISO2008to2015.pdf>
- Winters, Jr R.E. (2014). *A Review ISO 9001:2015 Draft - What's Important to Know Now*. Retrieved May 24, 2015 from: http://www.asrworldwide.com/images/Quality_Registrar/Presentations/ISO-Review/2015_ISO_9001_Review_Mar2014.ppt