SYSTEMS & MANAGEMENT
Electronic magazine

COMPARATIVE ANALYSIS BETWEEN ABNT NBR ISO 9001:2015 AND ABNT NBR ISO 31000:2009: THE RISK MINDSET IN QUALITY MANAGEMENT SYSTEMS

Victor Gomes Simão
victorsimao@yahoo.com.br
Fluminense Federal University - UFF, Niterói, Rio de Janeiro, Brazil.

Noemi Bonina
noemi_alice@yahoo.com.br
Fluminense Federal University - UFF, Niterói, Rio de Janeiro, Brazil.

Gilson Brito Alves Lima
glima@id.uff.br
Fluminense Federal University - UFF, Niterói, Rio de Janeiro, Brazil.

Osvaldo Luiz Gonçalves Quelhas
osvaldoquelhas@id.uff.br
Fluminense Federal University - UFF, Niterói, Rio de Janeiro, Brazil.

Marcelo Jasmim Meiriño
marcelojm@id.uff.br
Fluminense Federal University - UFF, Niterói, Rio de Janeiro, Brazil.

ABSTRACT

The new revision of the ISO 9001 standard was launched in 2015 and incorporated new concepts into its collection of requirements for the implementation of a quality management system, such as stakeholder relations, knowledge management, and risk management, broadening its scope of focus. In this sense, and predicting that changes will occur in organizations from this new perspective, this article aims to present the use of risk mentality in quality management systems, through a comparative analysis between the standards ABNT NBR ISO 9001:2015 and ABNT NBR ISO 31000:2009. The research is characterized as qualitative, and was conducted based on documentary research and systematic literature review. The findings suggest that the concept of risk-based thinking has always been implicit in ISO 9001, manifested in the form of preventive actions, and that the intention to incorporate risk thinking as a requirement in the 2015 version is to encourage organizations to take risk as a criterion in their decisions. It is evident that the risk and prevention literature is aligned with the most advanced quality management system methods, which are based more on prevention principles than on corrective actions.

Keywords: ISO 9001, ISO 31000, risk mentality, quality management systems (QMS).

PROPPI / LATEC
DOI: 10.20985/1980-5160.2019.v14n3.1430

Electronic Journal of Management & System
Volume 14, Number 3, 2019, pp. 310-322
DOI: 10.20985/1980-5160.2019.v14n3.1430

1. INTRODUCTION

The world has undergone significant transformations, either through the consolidation of practices and processes in organizations, or through the intensification of global interaction between economic and social agents. One of these consolidated concepts, increasingly practiced and disseminated, is the quality management approach.

Quality Management Systems (QMS) have been disseminated around the world since the 1980s, with the publication of the first edition of ISO 9001, which sets out the requirements that a quality management system must meet to be certifiable. ISO 9000 family standards define quality system standards that guide an organization's performance in terms of specific requirements (Bonina, 2009; Fonseca, 2015).

The globalization of the economy has made it necessary to standardize the requirements of quality assurance systems. The body that edits, reviews, and disseminates these standards is the International Organization for Standardization (ISO). It was established in 1947, is private, non-profit, and 162 countries in 210 Technical Committees that take care of the specific standardization of each sector of the economy are part of it. Each committee prepares international standards for its sector-specific products and services. (Fernandes, 2011).

The benefits gained from implementing quality management systems, whose primary objective is to demonstrate the ability of companies to deliver products and services that meet customer requirements, have been widely researched worldwide. Depexe and Paladini (2008) point out as benefits for certified companies the reduction of the number of complaints by customers, the reduction of delivery time, the improvement of the production process and the improvement of work processes and procedures. According to Bonina (2009), the standard does not establish how the requirements should be implemented, which represents flexibility and compatibility with any branch of activity, besides being a mechanism for obtaining competitive advantage among organizations from various sectors.

According to Nascimento (2016), on average, every five years ISO standards undergo a review process to determine whether they should be maintained, altered or discontinued in order to preserve the current and evolving organizational practices.

Thus, the version of ISO 9001/2008 has been included in this update process from 2013 and, according to the deliberations of the members of the ISO/TC176 Technical Committee, its content has been extensively reworked and the new revision was published in October 2015.

In the new version, this standard brought as major innovation the incorporation of the concepts of risk-based thinking and knowledge management, concepts that companies, currently certified, should adapt in order to keep up their quality management systems.

For Fonseca (2015), ISO 9001:2015 (ABNT NBR ISO 9001:2015 – Quality Management Systems – Requirements) represents a major source of problems for over 1 million companies, currently certified, and for many professionals in the field, due to the numerous conceptual novelties and the new requirements that have emerged in its content.

Incorporating new concepts in the QMS in organizations provokes new reflection on the adequacy of these practices to the organizational daily life, understanding that one of the biggest changes for these organizations will be to introduce knowledge management and risk-based thinking in their internal processes.

However, the author believes that the new standard will bring greater benefits to quality management systems, with less emphasis on documentation and new approaches that reinforce the context of the organization, risk-based thinking, and knowledge management, thus strengthening the path of organizations on their way to total quality. Such approaches are unprecedented in QMS, although they are already implicit in previous versions of the standard and other management systems, some of these concepts even appear in their own standards, such as risk management, which is represented by ISO 31000 (ABNT NBR ISO 31000:2009 – Risk Management – Principles and Guidelines), which justifies a more thorough analysis to understand how organizations adopting quality management systems based on ISO 9001 already dealt with these issues, as well as verified how these changes would impact the maintenance of existing systems.

In this context, the work aims to evaluate the impact that the change of focus of the ISO 9001 standard, in its 2015 version, may have on the quality management practices performed by the certified organizations, with emphasis on the insertion of risk-based thinking, which should guide companies' management activities and guide their quality management systems. In this sense, the objective of this article is to make an observation of the uses of risk mentality in ISO 9001 and ISO 31000 standards, besides presenting an example of the use of the interaction of these new concepts in organizations.

2. BIBLIOGRAPHIC REVIEW

2.1 The ISO 9001 Standard Review Process

Formed in 1979, the Technical Committee 176 (ISO/TC176) is responsible for Quality Management and Quality Assurance standards. Their latent concern was the increasing demands of different world markets, which, accompanied by the emergence of national consumer guarantee systems, were creating obstacles to the growth of international trade. (Nascimento, 2016).

In 1987, five international standards, known worldwide as the ISO 9000 Series standards, created to facilitate international trade and standardize quality management requirements around the world were edited and approved. The implementation structure of a quality management system follows the PDCA principle (Plan, Do, Check, and Action) (Bonina, 2009).

Vitoreli and Carpinetti (2013) state that the ISO 9001 standard is characterized for being generic and usable by any organization wishing to establish a QMS, with the possibility of certification by an external body.

The spread of this family of standards was so intense that, in November 1988 in the United States, the first Malcolm Baldrige Prize was awarded, while in Europe, in 1988, the European Quality Prize was instituted, and in Brazil, in 1991, the National Quality Award (PNQ) was created.

The ISO 9000: 1987 Series standards were first revised in 1994, and gave rise to the ISO 9000: 1994 Series standards (Fernandes, 2011). The 1994 revision of ISO 9001 brought more emphasis on product quality assurance than on company results, along with the emergence of awards for excellence in quality.

In the year 2000, the series was revised giving rise to the ISO 9000: 2000 Series standards. Aspects valued by the awards for excellence in quality were incorporated, that is, customer satisfaction, company results, business management, and continuous improvement. In December 2005, the ISO 9000: 2005 of Fundamentals and Vocabulary was launched and, in October 2008, ISO 9001:2008, in a revision that presented minor evolutions in relation to the previous version, keeping the focus on the aspects already raised by the revision of the year 2000 (Carpinetti, 2010; Fernandes, 2011; Nascimento, 2016).

A new revision of the ISO 9000 series is published in 2015 and in ISO 9001, this time, significant changes are found, showing that it brings maturity and broadening of concepts, as well as new approaches to the practice of continuous improvement.

Presenting the standard review process, the following topic addresses the 2015 revision of ISO 9001.

2.2 New approaches in the ISO 9001 revision 2015

The overall structure of the standard remains committed to the process approach, seeking interaction between outcome and strategic direction through the PDCA continuous improvement cycle that was designed by Shewhart in 1931. The PDCA cycle focuses on process analysis, problem solving, and standardization of routines, being widely used as a tool for continuous process improvement (Fonseca, 2015). In this respect, the standard broadens the scope of the process approach by incorporating the need to focus on the risk mindset to better seize opportunities and prevent undesirable outcomes.

The eight traditional quality management principles have also been revised and condensed into just seven principles (Box 1): customer focus, leadership, people engagement, process approach, improvement, evidence-based decision making, and relationship management. (ABNT, 2015). Both process and systemic approaches merge into one principle, whereas the process approach already implies considering a systemic view of the organization.

Chart 1. Changes in quality management principles

ISO 9001:2008	ISO 9001:2015
1. Customer Focus	1. Customer Focus
2. Leadership	2. Leadership
3. People involvement	3. People's Engagement
4. Process Approach	4. Process Approach
5. Systemic approach to management	5. Improvement
6. Continuous improvement	6. Evidence-based decision making
7. Fact-based decision making	7. Relationship Management
8. Mutual Benefits in Supplier Relations	

Source: Adapted from Fonseca (2015).

The new version of the standard seeks to provide requirements applicable to all sizes and types of organizations in any industry, with varying degrees of maturity of their management systems. A feature that has remained part of the norm is the customer-centric approach as key to business success, as companies need to adapt to meet growing customer needs by gaining and monitoring this feedback to meet their needs and expectations (Fernandes, 2011).

To meet the quality principles set out in the new review and to facilitate the demonstration of QMS requirements, seven sections were created: organization context, leadership, planning, support, operation, performance appraisal, and improvement (ABNT, 2015), as may be seen in Figure 1.

For Vitoreli and Carpinetti (2013), understanding the links between requirements is important for the construction of QMS (Figure 1). In this respect, the relationships between the sections of the new ISO 9001 review can be described starting from understanding the context of the organization and the objectives to be achieved, where top management assumes its leadership role, establishing the policy and responsibilities that will enable planning to achieve these objectives, as well as addressing appropriate risks and opportunities.

Only by structuring the context, policy and objectives (first stage of PDCA planning), the operationalization of meeting the requirements established by customers (second stage of execution of PDCA) is started, that is, all the support needed to operationalize the realization of the product and/or service (resources, dissemination forms, communication, information to be documented, operational control, design and development of products and services, among others) is provided. Upon completion, the product and/or service is delivered to customers and the organization must monitor their satisfaction as well as perform relationship management (PDCA verification step) so that they can have data to evaluate performance through the measurement of these indicators, audits and critical analysis, fostering continuous improvement of the quality management system and meeting the fourth stage of the PDCA (ABNT, 2015; Bonina, 2009; Carpinetti, 2010; Fernandes, 2011).

Some terminologies are reformulated to clarify the scope of the standard. Terms such as “exclusions” and “management representative” that were used until the 2008 version are no longer used in this new version as the applicability of requirements and definitions of responsibilities can be critically analyzed from the activity performed by organization and the nature of the risks and opportunities that are encountered by it (ABNT, 2015).

The terms “products and services” were differentiated to include everything that refers to the outputs of a process, emphasizing a peculiar characteristic of services, which is to have part of its output performed at the customer interface. This makes the standard more generic to facilitate its application by the service industry, and requirements that enhance confidence in an organization’s ability to deliver compliant products and services have been improved.

New concepts were also introduced in this review, aiming, according to Fonseca (2015), to bring more comprehensive practices from business excellence models to the requirements implemented and certified in quality management systems. In this sense, it deals with relationship management, performance evaluation, organizational knowl-

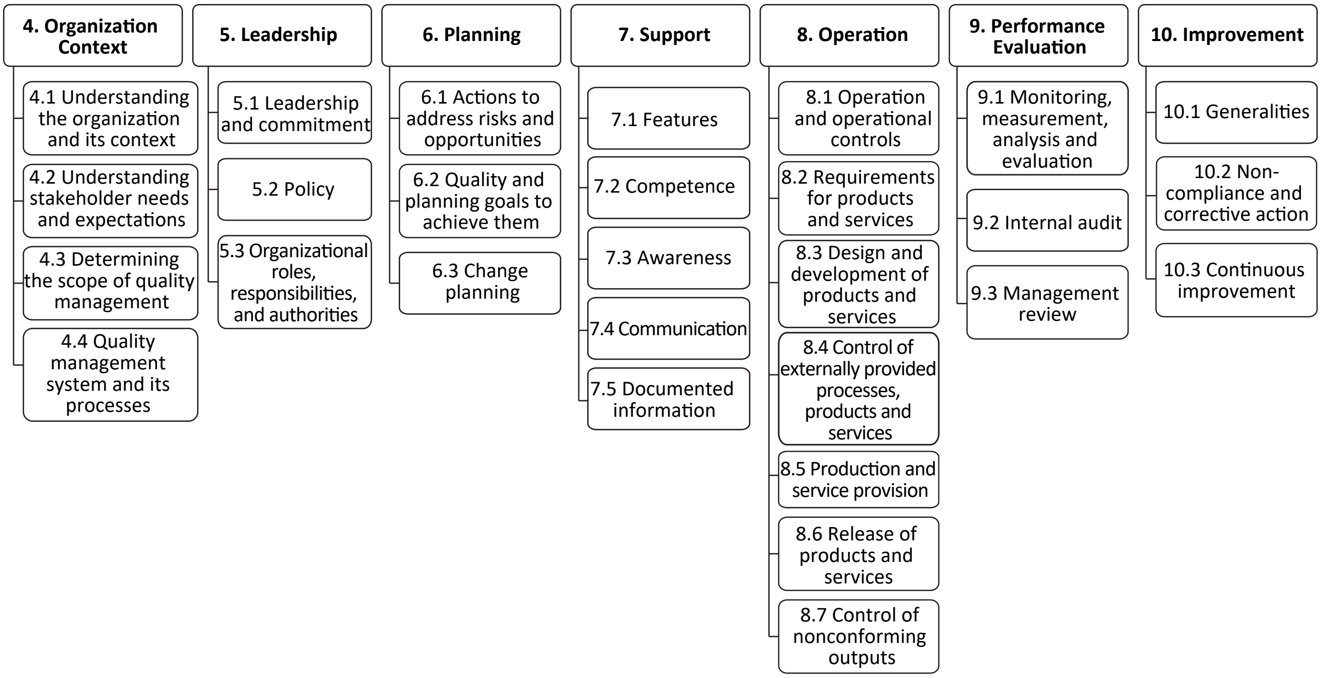
4. Organization Context
4.1 Understanding the organization and its context
4.2 Understanding stakeholder needs and expectations
4.3 Determining the scope of quality management
4.4 Quality management system and its processes
5. Leadership
5.1 Leadership and commitment
5.2 Policy
5.3 Organizational roles, responsibilities, and authorities
6. Planning
6.1 Actions to address risks and opportunities
6.2 Quality and planning goals to achieve them
6.3 Change planning
7. Support
7.1 Features
7.2 Competence
7.3 Awareness
7.4 Communication
7.5 Documented information
8. Operation
8.1 Operation and operational controls
8.2 Requirements for products and services
8.3 Design and development of products and services
8.4 Control of externally provided processes, products and services
8.5 Production and service provision
8.6 Release of products and services
8.7 Control of nonconforming outputs
9. Performance Evaluation
9.1 Monitoring, measurement, analysis and evaluation
9.2 Internal audit
9.3 Management review
10. Improvement
10.1 Generalities
10.2 Non-compliance and corrective action
10.3 Continuous improvement

Figure 1. Requirements of ISO 9001:2015

Source: Prepared by the authors.

Electronic Journal of Management & System
Volume 14, Number 3, 2019, pp. 310-322
DOI: 10.20985/1980-5160.2019.v14n3.1430

edge management and risk management, which promotes a change in the perspective on preventive action.

With regard to the context of the organization, its concept prescribes that the internal (culture, values, mission, vision, knowledge, etc.) and external (political, economic, social, technological, environmental, etc.) factors relevant to the scope of the strategic objectives and goals of the quality management system should be defined, as well as the concept of risk-based thinking, in which the organization must identify the risks and opportunities associated with its context and objectives.

Within this approach, two key risks must be considered: failure to deliver compliant products and services, and failure to achieve customer satisfaction. It is important to note that precautionary action requirements have been eliminated because with the change of approach, their need has been discontinued.

Also according to Fonseca (2015), ISO has introduced a text structure common to all its management system standards. The introduction of the concepts of opportunities and risks to the management system reinforces the use of ISO 9001 as an instrument that can help organizations create viable governance systems that can culminate in management excellence.

Through risk-based thinking for all its parts, the standard promotes a proactive approach to risk identification and seizes opportunities to feed the continuous improvement system. This issue is expected to lead to improvements in governance and decision making, facilitating the integration of multiple systems, which can tend to save time and money. (Fernandes, 2011; Fonseca, 2015).

In addition, the introduction of the concept of documented information, from which the organization defines what it will document, reinforces the idea that quality management systems are strategic and should strive for organizational knowledge management, no longer characterized by paper-based bureaucratic systems.

As a benefit to organizations, this new release provides the opportunity to review the organization and its current processes, leading to alignment with business strategy, to enhance the quality of products and services, and to achieve performance improvements that promote sustainability (Nascimento, 2016). Concepts have been expanded to an approach that should consider risks and opportunities as preventive action.

Following is one of the new concepts brought by the new version of ISO 9001, the risk mentality in the formulation of requirements of a QMS, which, within the perspective of the new revision, expresses the concept of preventive action. In this sense, the risk management perspective addressed by the 31000 standard is presented, in comparison with the formulation of risk mentality requirements in ISO 9001.

2.3 Risk requirements as part of the new ISO 9001 standard

The current version of ISO 9001 brings the concept of the risk mindset comprehensively into many of its requirements.

Considering that organizations are adaptive systems and, therefore, are constantly changing to meet market demands, seeking to standardize concepts and practices with a view to meeting customer requirements, as early as 2009, ISO issued a non-certifiable standard with the purpose of serving as a guideline for risk management principles and guidelines, ISO 31000 (ABNT NBR ISO 31000:2009 – Risk Management – Principles and Guidelines).

ISO 31000 provides recommendations on the principles and guidelines for implementing risk management in organizations. It is divided into three sections: principles, structure and process (Figure 2), and demonstrates the relationship between these three sections. The standard structure follows the PDCA guidelines, which facilitates the use of the standard to systematically implement risk management.

The risk mindset, according to ISO 9001 (ABNT, 2015), enables an organization to determine factors that could cause deviations in its processes and QMS from planned results, to put in place preventive controls to minimize adverse effects and maximizing the use of opportunities that arise. The risk mindset, according to ISO 9001 (ABNT, 2015), enables an organization to determine factors that could cause deviations in its processes and QMS from planned results, to put in place preventive controls to minimize adverse effects and maximizing the use of opportunities that arise.

According to ISO 9001:2015, “risk is the effect of uncertainty, and any uncertainty can have a positive or negative effect. A positive deviation from a risk may offer an opportunity, but not all positive risk effects result in opportunities.” (ABNT, 2015, p. xi). On the other hand, ISO 31000:2009 defines risk as the effect of uncertainty on objectives, which is the deviation from expected, and it may be positive and/or negative.

The ISO 9001 standard (ABNT, 2015) exemplifies that opportunities may arise as a result of a situation favorable to the achievement of an intended result, for example, a set of circumstances that enables the organization to adopt new practices, approach new customers, open new markets, developing new products, services, and technologies, building partnerships, and reducing waste or improving productivity.

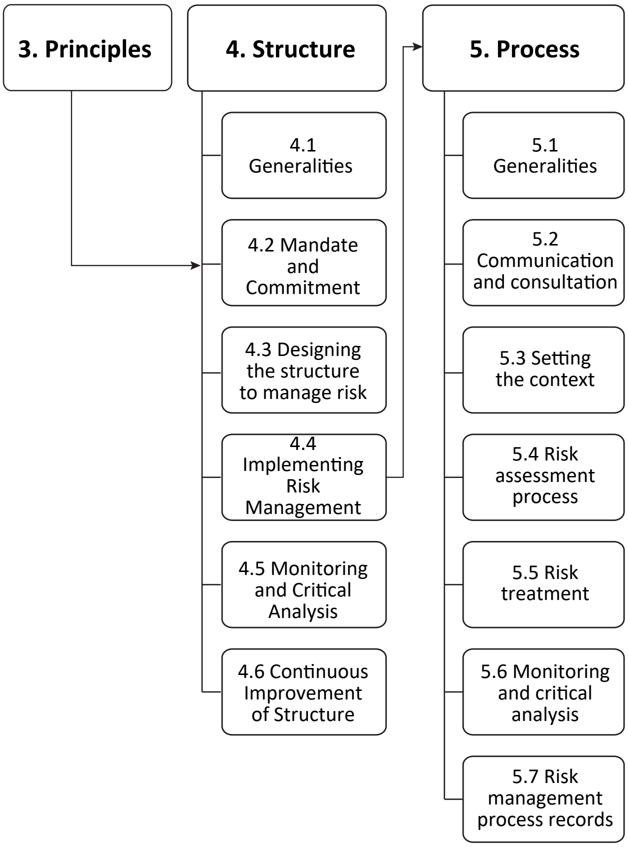
3. Principles
4. Structure
4.1 Generalities
4.2 Mandate and Commitment
4.3 Designing the structure to manage risk
4.4 Implementing Risk Management
4.5 Monitoring and Critical Analysis
4.6 Continuous Improvement of Structure
5. Process
5.1 Generalities
5.2 Communication and consultation
5.3 Setting the context
5.4 Risk assessment process
5.5 Risk treatment
5.6 Monitoring and critical analysis
5.7 Risk management process records

Figure 2. ISO 31000:2009 Requirements

Source: Prepared by the authors.

Actions to address opportunities also include consideration of associated risks. Thus, the concept of opportunity associated with the positive outcome of a risk, in a way, came as an extension of the concept of improvement through preventive actions.

In the management of QMS processes within the PDCA cycle principles (Liebesman, 2005), the focus on risk mindset is now included.

Organizations will need to plan and implement actions to address risks and opportunities and this new form of action aims to take advantage of opportunities and prevent undesirable outcomes. The risk and opportunity approach lays a foundation for increasing the effectiveness of the quality management system, achieving improved results and preventing negative effects.

Operationally, it is noted that ISO 31000 (ABNT, 2009) defines the risk assessment macroprocess as one that encompasses the steps of risk identification, analysis and assessment, where risk identification aims to generate a comprehensive list of all possible risks, based on events that may create, increase, avoid, reduce, accelerate or delay the achievement of objectives.

Risk analysis involves understanding risks and assessing their consequences and probabilities. Depending on the circumstances, the analysis may be qualitative, semi-qualitative or quantitative, or a combination of these. Regarding risk assessment, ISO 31000 (ABNT, 2009) states that at this stage the comparison between the level of risk found during the previous process and the established risk criteria occurs. Based on this comparison, the need and priority of treatment can be defined (Ferreira *et al.*, 2014).

According to the leadership principle defined in ISO 9001 (2015), top management continues to hold responsibility for the QMS. The standard defines that senior management must demonstrate leadership and commitment to the quality management system, be accountable for its effectiveness and promote the use of the process approach and risk mindset, in addition to demonstrating commitment to customer focus by ensuring that risks and opportunities that may affect product and service compliance and the ability to increase customer satisfaction are determined and addressed.

Bringing a new reading of concepts that have already been addressed in ISO 31000 (ABNT, 2009), ISO 9001 (ABNT, 2015) presents the concepts of stakeholders and organizational context as necessary prerequisites for the correct definition of risks and opportunities. According to ISO 31000, when setting a context, the organization articulates its objectives and defines the external and internal parameters to be taken into consideration. When managing risks, the scope and risk criteria for the rest of the process should be established. In addition, the organization should define the criteria to be used to assess the significance of the risks, the objectives it intends to achieve, and the external and internal factors that may influence this search (Ferreira *et al.*, 2014).

When planning QMS, the organization should consider its context and stakeholder relationship to determine the risks and opportunities that need to be addressed to ensure that the system can achieve its intended outcomes, increasing desirable effects and preventing or reducing undesirable effects.

This requires action planning to address these risks and opportunities, integrating and implementing actions in the company's QMS processes, and evaluating the effectiveness of those actions taken to address risks and opportunities, which should be appropriate to the potential impact on product and service compliance.

According to Ferreira et al. (2014), at the risk treatment stage, the ISO 31000 standard provides for the assessment of the treatment of already materialized risks. Such decision includes the decision-making process of a management system that should classify and define whether its residual risk levels are tolerable; and if the implementation of a new treatment for risks is necessary in case these levels are not tolerable, as well as the assessment of the effectiveness of such treatment.

Thus, in selecting the most desirable risk treatment option, the organization should balance costs and efforts to implement treatment systems on the one hand, and benefits arising from legal, regulatory, social responsibility, and protection of the natural environment, among others.

As possible options for dealing with risks, ISO 9001 also appropriates the concepts defined in the specific standard, providing options for addressing them that include alternatives to avoid risk, take risk to pursue an opportunity, eliminate the source of risk, change the likelihood or consequences, share the risk or decide to retain the risk based on information and evidence.

According to the steps of the PDCA cycle, as risk-related improvement actions, ISO 9001:2015 states that the organization shall analyze and evaluate appropriate monitoring data and information and these results shall be used to assess the effectiveness of actions taken to address risks and opportunities (Nascimento, 2016). The points of monitoring and measurement necessary for control are naturally specific to each process and vary depending on the related risks.

For Liebesman (2005), preventing is better than correcting, and for good corporate governance, the main goals are risk management, effective process management and continuous improvement of company performance. The direction of the organization must change the corporate mindset from problem correction to prevention.

Liebesman (2005) mentions that the Sarbanes-Oxley Act brought the need to better identify and manage corporate risk. Quality management and environmental management systems are tools that can interact with the actions proposed by risk management, insofar as the risky operating situations are foreseen by the senior management of the organization and disseminated to all levels.

Certainly, the organizations currently performing QMS certification activities should be adapted to the new demands of organizations, be qualified and able to evaluate risk management systems, and be part of the quality management systems. This change tends to create a new frontier for the training of auditors and evaluators, which will require much more extensive and comprehensive training.

3. RESEARCH METHODOLOGY

This study is characterized as a descriptive conceptual theoretical work on a certain theme (Zago and Retour, 2013), which presents a systematization of a bibliographic and documentary research, through a critical analysis.

This is a qualitative research that presents a bibliographic review about the history of revisions of ISO 9001, as well as the tools used by companies for risk management, through examples and representations of the integration between ISO 9001:2015 and ISO 31000:2009.

The methodological process aims to give robustness to a scientific research and for this it is essential to choose the one that sustains and structures the research in what it is intended to observe (Zago and Retour, 2013).

In this sense, an exploratory and descriptive research was developed. It was sought to use the bibliographic and documentary research to perform data collection, considering it to be an appropriate method to make the observations relevant to this work.

Given the proposed objectives of evaluating the impact of the insertion of risk-based thinking in the quality management practices of organizations that operate in line with the requirements of ISO 9001, it was decided to carry out a bibliographic research that would show the confluence between these themes in academic literature in recent decades.

Thus, it was sought to identify works that specifically address the issue of risk management, in strict relation to quality management, to give a more precise theoretical basis for this research (Table 2).

Therefore, a bibliographic survey was conducted in the databases of articles and academic journals Scopus and Portal Capes. In order to seek the widest possible range of publications already made on the two themes in question, Chart 2 listed the keywords used in the search: “ISO 9001” and “Risk Management” and the results found in each database, respectively.

4. DISCUSSION OF RESULTS

The literature review shows that the culture of risk management is a multi-dimensional concept that will lead companies that want to maintain their quality management systems and implement process improvements to reduce their level of defective products, customer satisfaction, employees and various stakeholders, reducing negative risks and risks that, while positive, do not represent an opportunity as a new way to strive for excellence.

The literature review shows that the culture of risk management is a multi-dimensional concept that will lead companies that want to maintain their quality management systems and implement process improvements to reduce their level of defective products, customer satisfaction, employees and various stakeholders, reducing negative risks and risks that, while positive, do not represent an opportunity as a new way to strive for excellence.

For this reason, environmental and occupational health and safety management systems have become quite common over the last 20 years, and environmental and safety management practitioners are often concomitantly members of the quality teams. This enhances the use of the risk mindset by ensuring that quality management goes hand in hand with risk management.

The actions taken to achieve continuous quality improvement are the same as those required to achieve effective organizational risk management, enabling the insertion of risk-based thinking in ISO 9001 and making its implementation compatible with risk management principles and guidelines already identified in ISO 31000:2009.

4.1 The risk mindset under the new ISO 9001 standard

The concept of risk-based thinking has always been implicit in ISO 9001, manifested in the form of preventive actions to eliminate potential nonconformities, and in analyzing the causes of nonconformities to prevent their recurrence.

For Nascimento (2016), what is intended is that organizations incorporate their concept and adopt risk as a criterion in their decisions. To assist in the implementation of a risk management system, there are other non-certifiable ISO standards that guide this implementation.

To apply risk-based thinking, the organization must have a clear idea of its context and objectives.

One of the purposes of a QMS is to act as a preventive tool, and risk-based thinking allows the organization to determine factors that may have the potential to lead its processes and QMS to deviations from planned outcomes to put in place preventive controls so as to minimize the negative effects and make the most of any opportunities that may arise.

In the new version of the standard, the concept of preventive action is expressed through the application of risk-based thinking. Its application in ISO 9001 allowed a reduction in prescriptive requirements and their replacement with performance-based requirements.

While specifying that the organization should plan actions to address risks, there is no requirement for formal methods for risk management practices or a documented risk management process.

Not all QMS processes represent the same level of risk in terms of the organization's ability to achieve its objectives, and the effects of uncertainty are not the same for all organizations. ISO 9001 defines that the organization is responsible for applying the risk mindset and the actions it takes to address risks, including the retention or otherwise of documented information as evidence of its risk determination.

Organizations may decide whether or not to develop a more comprehensive risk management methodology than that required by the standard, for example by applying other guidelines or standards.

In comparison, ISO 9001:2015 rescues the risk treatment options described in ISO 31000 (2009), which may include: avoiding risk (avoiding concept), taking risk in order to seek an opportunity (accepting concept), eliminating the source of risk by changing the probability or consequences (mitigating concept), sharing the risk (transferring concept), or retaining the risk based on informed decision (accepting concept).

The relationship found between the two standards can be built from some specific requirements, in order to facilitate the understanding and application of concepts in the practice of organizations.

4.2 Using the risk mindset in quality management systems

Interrelating can represent the least laborious way to implement the risk mindset in a construction process, or QMS adequacy, by looking at the scenarios and context of the implementation.

By way of illustration of practical application, one of the elements that require the most attention when an organization implements its QMS is the requirements, as they address the operation of organizations; and they are represented in item 8.0 of ISO 9001: 2015. To this end, a framework has been prepared to illustrate the interrelationship between standards (Table 3), to be based on the requirement "8.4 - Control of externally provided processes, products and services".

Considering the external and risk management contexts, and the responsibilities of top management (governance) and managers at other levels of organizations (operations and activities), the relationship between these aspects can be seen in Chart 3.

Chart 2. Bibliographic survey and main results found

Search conducted at Scopus portal			Keywords cited													
Author	Year of publication	Search Title	Quality control	Management system	Quality management systems (QMS)	Occupational Health and Safety Management System (OHSMS)	Total Quality Management	ISO 9001	Environmental management systems (EMS)	Risk Management	Sustainability	Maritime safety regulations	Risk management	Strategic planning	Industrial management	Regulatory compliance
Liebesman, S.	2004	Quality Practitioners and Effective Corporate Governance		x	x								x	x		
	2005	Mitigate SOX risk with ISO 9001 and 14001														
	2005	Compliance and ethics group formed	x										x	x	x	x
Celik, M.	2009	Establishing an Integrated Process Management System (IPMS) in ship management companies			x			x		x		x				
	2009	Designing of integrated quality and safety management system (IQSMS) for shipping operations			x			x		x		x				
Baldassarre, M.T.	2012	Harmonization of ISO/IEC 9001: 2000 and CMMI-DEV: From a theoretical comparison to a real case application						x								
	2013	A strategy for painless harmonization of quality standards: A real case			x	x		x								
	2014	A reference ontology for harmonizing processreference models														
Santos, Gilberto	2013	The main benefits associated with health and safety management systems certification in Portuguese small and medium enterprises post quality management system certification			x	x		x								
	2014	Conception of a flexible integrator and lean model for integrated management systems			x	x			x							
Gołaś, Hanna	2014	Risk Management as Part of the Quality Management System According to ISO 9001			x			x		x						
Fonseca, L. M.	2014	ISO 9001:2015 Revision		x	x			x								
	2015	ISO 14001:2015: An improved tool for sustainability							x		x					
	2015	FROM QUALITY GURUS AND TQM TO ISO 9001:2015: A REVIEW OF SEVERAL QUALITY PATHS		x	x		x	x								

Source: Prepared by the authors.

In the external context, opportunities and threats to governance, operations and activities are observed.

In this perspective, top management can address the opportunities and threats for promoting good governance through strategic planning correlated with compliance with requirement 8.4.1 - generalities as set out in ISO 9001, as well as setting targets, values and objectives should be interrelated with the objectives for risk criteria (Table 3).

For senior management, it is essential to consider the external and risk management contexts in joint action to promote the development of a consistent, effective and efficient governance policy, supported by decision support strategies (Figure 3).

In the elaboration, implementation and execution phase of the activities, which is under the responsibility of the operational managers, compliance with the assumptions of both risk and external contexts must be considered. To this end, management can work the requirements of both standards together, as shown in Table 3.

The pursuit of the implementation of ISO 9001 may be better suited to the reality of the organization when it seeks to ascertain the degrees of QMS compliance with risk management requirements.

Figure 3 represents how risk management is intrinsically related to decision making in organizations, as building a risk mindset that is in accordance with decision levels (procedural, operational, strategic) is critical in each part of the process.

Chart 3. Practical Applications ISO 9001:2015 x ISO 31000:2009

Applied to ISO 9001 Item 8.4: Process Control and Externally Provided Products	Normative reference	**External context**		**Risk Management Context**
		Opportunities and Threats	Values, goals and objectives	Risk Management
Governance (top management)	ABNT NBR ISO 31000	Strategic planning	Objectives (and risk criteria policy) (4.3.2)	Structure Design for Risk Management (4.3)
	ABNT NBR ISO 9001	8.4.1 - Generalities	8.4.1 - Determine and apply criteria for evaluation, selection, monitoring and reassessment of external providers.	8.4.2 - Control Extension Type
Operations and activities (all managers)	ABNT NBR ISO 31000	Strategic planning 8.4.1 - General 5.3.4 - Setting the context of the risk management process Daily decisions to execute the plan	Risk Criteria (5.3.5) are based on the external and internal contexts of the organization.	5.4 - Risk Management Processes
	ABNT NBR ISO 9001	8.4.3 - Information for external providers - Items a, b, c.	8.4.3 - Information for external providers	8.4.3 - e) control and monitoring of external provider performance. 8.4.3 f) verification or validation activities.

Source: Prepared by the authors.

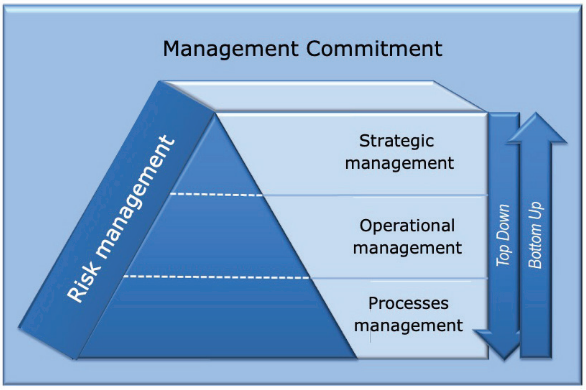

Figure 3. Risk management in decision support

Source: Prepared by the authors.

Risk management must go through all decision-making phases that imply commitment to the management of organizations, as each decision and activity level assumes its inherent risks.

In a typical hierarchical pyramid, decisions start from top to bottom and unfold according to the range of action of each level.

On the other hand, to make fact-based decisions, it is important that information is bottom-up, and throughout the process, building responses will be provided as a decision input for the organization to fulfill its role. This information evolves and the incorporation of new information along the bottom-up flow provides the construction of knowledge to strengthen decision making, in a cyclical process of fostering decision making from the generated knowledge.

Thus, models such as "top-down" and "bottom-up" operationalize the generation of organizational knowledge necessary to define risks and opportunities from the context of the organization.

For Wanke (2008),

> "Within organizations, each approach may, individually, be more in line with a given planning horizon and/or type of decision making. For example, the top-down approach tends to be employed over longer time horizons and for more aggregated data, while the bottom-up approach tends to be more adopted over shorter time horizons and for individual items. " (p. 231).

Top-down and bottom-up models, although from different perspectives, are collaborative with risk assessment, which facilitates risk management (Figure 3) and maximizes the use of opportunities that minimize deviations in the processes and, consequently, in the QMS, in relation to the planned results.

For Nonaka and Takeuchi (2008), in the top-down management model, the knowledge that is generated by top management goes on to be processed and implemented.

In the bottom-up model, in turn, frontline employees create knowledge from some top management signals, but more often than not they are entrepreneurial employees.

According to Nonaka (2001, p. 43), "frontline employees are immersed in the daily details of specific technologies, products or markets. No one understands as much as they do the reality of the company's business. "

Top-down models are aggregate element prediction models, as reinforced by Jakobsson et al. (2014), such as macroeconomic systems and models. Bottom-up models are representative models of chains and operational prevention systems.

The first model fits in with the process of capturing the organization's objectives and the diversity of risk criteria, considering that for effective risk management the needs and risk criteria specific to each sector must be analyzed according to their specificity.

Within this perspective, improving governance, organizational learning, and stakeholder confidence, as well as establishing reliable foundations for decision making and planning, given that these are some elements that underpin the implementation of risk management throughout the organization, the adaptation of the top-down model is an alternative that may be strategic for top management work.

Practices such as improving controls, efficiency, and operational effectiveness, proactive management, use of risk management resources, loss prevention and minimization, and also the "development of standards, guidelines, procedures and codes of practice that, in whole or in part, establish how risk should be managed within the specific context of these documents" (ABNT, 2009, p. v), would be appropriate to the propositions associated with bottom-up model adjustments.

Although each model occurs at different times in the risk identification process, when analyzed from the objective of creating the risk mentality in organizations, they are complementary to the construction of a solid risk management structure.

ISO 31000 (2009) adds activities to expressions in order to clarify understanding by organizations. Thus, it considers the reference to the architecture to manage risks - principles, structure and process, such as "risk management", and the application of this architecture is presented using the term "managing risks".

Figure 3 shows that risk management runs through all the organization's processes and that their identification, implementation and maintenance correlate interdependently with models that fit the needs of each organization's specificities.

Relating the expressions to the models presented and considered complementary, even when implemented at different times in organizational life, "risk management" can be correlated to top-down, as it presents the structure that will provide the foundations for incorporating risk management at all levels of the organization and "managing risk" at bottom-up, including the risk assessment, treatment and monitoring process.

As with quality management, quality policy definitions and objectives are closer to the top-down model. Performing the organization's purpose activities, operating procedures for the realization of products and services, analysis, measurement and monitoring controls, as well as meeting customer expectations would meet the bottom-up model.

Finally, the implementation of a risk-minded quality management system assumes that the interrelationships between different concepts are well analyzed so that they can generate effective results, regardless of the perspective of efficiency and effectiveness in the practices and processes adopted by the organizations.

5. FINAL CONSIDERATIONS

The theoretical survey made in this research allowed the definition of some fundamental basic assumptions for updating the QMS based on the new revision 2015 of ISO 9001.

In applying the concept of risk-based thinking, the organization should identify the risks and opportunities associated with its context and objectives, plan how to integrate and implement actions to address these risks and opportunities within its management system processes, and evaluate the effectiveness of these actions to ensure that the QMS can achieve the desired results, improve the desirable effects, prevent or reduce unwanted effects, and achieve improvements.

Actions to address risks and opportunities as new requirements need to be addressed with caution, as the possibilities for identifying risks and opportunities within any organization are numerous. The company must have a clear idea of its context and objectives so that it can properly define and program the guidelines, methodology and criteria against which it will analyze, prioritize, and address the associated risks and opportunities.

Actions to address risks and opportunities should be commensurate with the potential impact of each identified risk on product and service compliance.

The new version of ISO 9001 does not require the organization to implement a risk management system as described in ISO 31000, but the organization may decide whether or not to develop a more comprehensive risk management methodology than required by the standard through the use of other methodologies or guides available.

The basic underpinning of a certification system should be the trust and reputation of the organizations involved in the certification of management systems, both those performing the evaluators' role and those being evaluated. The key words for the success of these systems are credibility and trust. And the new approaches to ISO 9001 will require much more training from their evaluators, pushing the boundaries of a standard.

Observing the scenario and the application and implementation context of the 9001 standard facilitates the incorporation of elements that make up the risk mentality. Moreover, seeking understanding of risk management relationships at each decision level can contribute to a more effective implementation of the quality management system by organizations.

This research sought to perform a theoretical comparative analysis between the quality management system standard (ISO 9001) and the risk management standard (ISO 31000), both edited by ISO, where the former was revised in October 2015, and the second has been in force since 2009. It was sought for this analysis some suggestions for organizations to observe the context and the scenario in the implementation of the new version of 9001, and to consider the aspects inherent in each level of decision, in order to encourage the practice of risk mentality in their relational environments.

Finally, it is understood that quality management systems can incorporate risk management very effectively as an induction mechanism to the continuous improvement of products, processes and services offered by organizations and mitigate the negative impacts that their processes may cause to the parties involved in the business of the organization.

To this end, it is important for interested organizations to delve deeper into the study of risk management through the most diverse methods; therefore, the ISO 31000 standard is a natural and simpler way for this process, given the similarity of its structure to other ISO standards for management systems.

Monitoring, measuring and observing how the implementation of the new version of ISO 9001 occurs, for example, considering companies' restructuring of concepts such as risk mentality, will represent future deepening for the research that follows in this direction.

REFERENCES

Associação Brasileira de Normas Técnicas – ABNT (2009), ABNT NBR ISO 31000:2009, *"Gestão de riscos – Princípios e diretrizes"*, ABNT, Rio de Janeiro.

Associação Brasileira de Normas Técnicas – ABNT (2015), ABNT NBR ISO 9001:2015, "*Sistemas de gestão da qualidade – Requisitos",* ABNT, Rio de Janeiro.

Bonina, N. (2009), *"A Qualidade Total no Serviço Público: os caminhos de uma instituição pública portuguesa rumo à certificação ISO 9001:2000*", Dissertação de Mestrado em Gestão de Recursos Humanos, Coimbra: ISMT-ESAE.

Carpinetti, L. C. R. (2010), *Gestão da Qualidade: conceitos e técnicas*, São Paulo, Atlas.

Depexe, M. D.; Paladini, E. P. (2008), *"Benefícios da implantação e certificação de sistemas de gestão da qualidade em empresas construtoras", Revista Gestão Industrial,* Vol. 4, No. 2, pp. 145-161.

Fernandes, W. A. (2011), *"O movimento da qualidade no Brasil", Essential Idea Publishing*, Rio de Janeiro – RJ.

Ferreira, R. O.; Lima, G. B. A. L.; Maciel, G. F. S. V. et al. (2014), *"Análise da implantação do processo de gestão de riscos com base na ISO 31000: aplicação numa empresa de energia", Relatórios de Pesquisa em Engenharia de Produção*, Vol.14, No. 13, p.159-172.

Fonseca, L. M. (2015) "ISO 9001 Quallity Managementt Syystemss through the Lenss *off Organizational Culture", Quality Management*, Vol. 16, No. 148, Oct, p. 63 - 78.

Fonseca, L. M. (2015), *"From Quality Gurus and TQM to ISO 9001:2015: A review of several quality paths", International Journal for Quality Research*, Vol. 9, No. 1, pp. 167–180.

Jakobsson, K.; Söderbergh, B.; Snowden, S. et al. (2014), *"Bottom-up modeling of oil production: A review of approaches", Energy Policy*, Vol. 64, pp. 113–123.

Liebesman, S. (2005), *"Mitigate SOX Risk with ISO 9001 and 14001", Quality Progress.* September.

Nascimento, L. C. (2016), *"A ISO 9001 vai mudar: O que você precisa saber – oficialmente".* ABNT/CB-25, 2013, Disponível em: http://www.ABNTcb25.com.br/ Acesso em: 12 jan. 2016.

Nonaka, I. (2001), *"A empresa criadora de conhecimento", In: HARVARD BUSINESS REVIEW. (Org). Gestão do Conhecimento*. Campus, Rio de Janeiro, p. 27 – 49.

Nonaka, I.; Takeuchi, H. (2008), *"Gestão do Conhecimento"*, Bookman, Porto Alegre.

Vitoreli, G. A.; Carpinetti, L. C. R. (2013), *"Análise da integração dos sistemas de gestão normalizados ISO 9001 e OHSAS 18001: estudo de caso múltiplos", Gestão & Produção,* São Carlos, Vol. 20, No. 1, pp. 204-217.

Wanke, P. (2008), *"Previsão top-down ou buttom-up? Impacto nos níveis de erros e de estoques de segurança", Gestão & Produção*, São Carlos, Vol. 15, No. 2, p. 231-245.

Zago, C. C.; Retour, D. (2013), *"Cultura organizacional: Nível coletivo constitutivo da gestão por competências", Gestão & Produção*, São Carlos, Vol. 20, No. 1, p.180-191.

Received: May 26, 2018

Approved: September 16, 2019

DOI: 10.20985/1980-5160.2019.v14n3.1430

How to cite: Simão, V. G.; Bonina, N.; Lima, G. B. A., et al. (2019), "Comparative analysis between ABNT NBR ISO 9001:2015 and ABNT NBR ISO 31000:2009: the risk mindset in quality management systems", Sistemas & Gestão, Vol. 14, No. 3, pp. 310-322, available from: http://www.revistasg.uff.br/index.php/sg/article/view/1430 (access day month year).