ISSN 1980-5411 (On-line version)
Production, 31, e20210036, 2021
DOI: 10.1590/0103-6513.20210036

Thematic Section - Future of Energy-efficient Operations and Production Systems

From theory to practice: a risk management model for SMEs in the context of ISO 9001

Yasmin Silva Martins[a], **Carlos Eduardo Sanches da Silva**[a], **Juliana Helena Daroz Gaudencio**[a]

[a]Universidade Federal de Itajubá, Itajubá, MG, Brasil

*yasminsm@unifei.edu.br

Abstract

Paper aims: To fulfill risk-based thinking (RBT), most companies opt for widespread methods as FMEA, even with their limitations. This research aims to develop a model for small and medium-sized enterprises (SMEs) relying on literature, practical and normative aspects, to accomplish RBT required by ISO 9001:2015.

Originality: This study represents an original contribution once its analysis and results guide a highlighted need in the literature. By discussing RBT from three different perspectives, this paper provides relevant insights for researchers and practitioners in quality and risk management.

Research method: The action research was conducted within a Brazilian SME, where the risk management model was implemented and analyzed through five cycles. The techniques to collect data were participant observation, documentary analysis, and semi-structured interviews, analyzed through attribute agreement analysis.

Main findings: Unlike the isolated use of widespread methods, this model contains all the aspects needed for RBT. Its applicability is directly related to the level of experience on risks and ISO 9001, emphasizing the organizational aspects needed.

Implications for theory and practice: A comprehensive model allows SMEs to understand better the concepts associated with RBT while incorporating an adapted approach to their contexts. Researchers can use the model to analyze its applicability for SMEs from different contexts.

Keywords

Quality management system. ISO 9001:2015. Risk-based thinking. Risk management. Action research.

How to cite this article: Martins, Y. S., Silva, C. E. S., & Gaudencio, J. H. D. (2021). From theory to practice: a risk management model for SMEs in the context of ISO 9001. *Production*, *31*, e20210036. https://doi.org/10.1590/0103-6513.20210036.

Received: Apr. 30, 2021; Accepted: Sept. 20, 2021.

1. Introduction

Small and medium-sized enterprises (SMEs) perform an extreme role in the economy of countries worldwide (International Organization for Standardization, 2016). The search for certification in ISO 9001, as a basis for the structuring of a Quality Management System (QMS), is a practice used by SMEs as well as companies of the most diverse segments and sizes, as a way to ensure adequacy and effectiveness in their activities, processes, services, and products (International Organization for Standardization, 2019; Fonseca, 2015; Anttila & Jussila, 2017). ISO 9001:2015 has incorporated significant and challenging changes in its latest update, such as the concept of risk-based thinking (International Organization for Standardization, 2015; Rampini et al., 2019). However, the standard does not indicate how the new requirements should be addressed by each organization, leaving them the decision of what is more appropriate to their context (International Organization for Standardization, 2015; Fraser & Simkins, 2016; Ezrahovich et al., 2017; Vasile, 2017; Anttila & Jussila, 2017; Perdigão et al., 2017).

Knowledge about risk management is a fundamental aspect in implementing any risk approach. However, it is possible to observe that many companies, both small, medium, and large, consider themselves unprepared for this implementation (Rybski et al., 2017). Fonseca & Domingues (2018), in a survey with SMEs from Portugal, identified that, for most of these companies, the implementation of a risk approach that meets the requirements of risk-based thinking is one of their biggest challenges. At the same time, the SMEs consider it one of the most beneficial requirements from the standard.

According to Crovini et al. (2021), the lack of procedures and strategies for risk management is related to the lack of risk mindfulness and knowledge. Since no specific methods and models are defined, most companies opt for widespread approaches. Martins & Silva (2019) identified, in their literature review, that most publications present proposals or applications of ISO 31000 (based on the PDCA cycle - Plan, Do, Check and Act) and the FMEA (Failure Modes and Effects Analysis), as a way to meet ISO 9001:2015. However, the authors point out that, before choosing to use such approaches, it is necessary to be aware of the limitations related to its isolated use.

In this context, there is an important gap in the literature, evidenced in the studies of Crovini et al. (2021), Fonseca et al. (2019), Martins & Silva (2019), Fonseca & Domingues (2018), Rybski et al. (2017) and Chiarini (2017). From the researches, the gap regards practical guidance on how to implement risk-based thinking, following the ISO standard effectively, once most SMEs do not implement appropriate techniques, presenting a biased view of the risk management process. Crovini et al. (2021) highlight the need for researchers to assist SME owners in understanding the importance of risk management in a structured and integrated manner, suggesting the use of participatory and active research and emphasizing that these methodologies can support scholars in spreading a proper business and risk culture.

The main objective of this paper is to address the mentioned gap, contributing with the scientific community and SMEs, through the development of a model for risk approach, based on the theoretical aspects identified in the literature and, also, in practices associated with its implementation in a Brazilian SME. The adequacy of the proposed model is analyzed within the study object through five action research cycles, with evaluations of internal and external specialists. The authors analyzed the evaluations obtained through interviews, with the agreement by attributes analysis, to ensure the adequacies proposed by the respondents for the systematic and their consistency with the defined standard evaluator.

This article is structured as follows: In the first section, the authors present a contextualization of the research problem and a definition of the objectives; then, in the literature review, there is an overview of the existing discussions on the subject and some concepts relevant to the study; the following sections discuss the development of the study, presenting the research methodology, findings and discussion and, finally, the research implications, followed by the conclusions with theoretical and managerial contributions and suggestions for future work.

2. Literature review

The systematic literature review (SLR) is a method used by many researchers to manage the diversity of knowledge by mapping and assessing existing intellectual territory (Tranfield et al., 2003). To conduct an SLR, researchers must follow a process of problem formulation, by defining a well-targeted research question; searching for articles by defining inclusion and exclusion criteria; data evaluation and analysis; and presentation of results (Arksey & O'Malley, 2005; Cooper, 1998).

In this study the authors based on their previous research, considering the following criteria: the search was conducted in Scopus and Web of Science, the most used databases, due their comprehensiveness, refinements, quality and accessibility (Mongeon & Paul-Hus, 2016; Li et al., 2010; Testa, 1998); between 2008 to 2019, in order to include documents published during the validity and transition of the version from 2008 to 2015, of the ISO 9001 standard; using "risk" and "ISO 9001" as keywords, as a way to generalize the terms, finding the largest possible number of documents related to the theme. The 58 papers selected were analyzed according their relation to the requirements of ISO 9001:2015, especially the ones related to risk-based thinking, serving as basis to the proposal of the risk management systematic. Moreover, the selected papers were used to structure this section, contextualizing the concepts that are more relevant for this study.

2.1. Small and medium-sized enterprises

Small and medium-sized enterprises represent more than 95% of all companies globally and play a vital role in the world's economies (International Organization for Standardization, 2016). Although they are more vulnerable to market failures and policy inefficiencies (Cusmano et al., 2018), SMEs tend to pursue higher-risk

strategies that do not usually exploit their innovation potential to the fullest. On the contrary, in large firms, owners are more likely to reconcile more comprehensive strategies in innovation with reduced risk (Maron et al., 2019). According to Crovini et al. (2021, p. 119), "[...] running a small business is particularly risky".

Small companies have some restrictions, such as financial and human resources, leadership issues, accumulation of requirements in various processes, and preliminary risk assessment (Zimon, 2016); in this context, the implementation of ISO 9001 in SMEs is a strategic decision. In addition to that, the lack of knowledge about risk management makes the implementation of any method, methodology, or tool difficult and its effectiveness compromised (Rybski et al., 2017).

Some authors, such as Cicek (2018), Jagodzi□ska (2018), and Chiarini (2017), point out that SMEs have more difficulty in adopting and implementing appropriate approaches for risk management. According to the authors, most of these companies do not have sufficient experience in this type of management, even though they are more exposed to negative aspects of risks. However, while small businesses consider the risk approach required by ISO 9001:2015 to be one of the most challenging requirements, they see their implementation as one of the most beneficial practices for companies (Fonseca & Domingues, 2018).

2.2. ISO 9001:2015 standard

The need to standardize procedures, reducing barriers to internationalization, increasing efficiency and involving various stakeholders, especially the customers, led to the creation of the ISO 9000 series standards (Perdigão et al. 2017), globally managed by the International Organization for Standardization (ISO) (Oliveira et al., 2011). The NBR ISO 9001:2015 was published in September of the same year, with two main objectives: reliability and flexibility (Fonseca & Domingues, 2018).

Some of the main changes in the standard include more emphasis on processes, reducing the documentation required; analysis of the organizational context and stakeholder requirements, to align the strategic direction; organizational knowledge management; change analysis; greater involvement of top management; and risk-based thinking, mentioned in most of the requirements of the standard, as a request for the entire organization (Fonseca, 2015; International Organization for Standardization, 2015; Chiarini, 2017; Vasile, 2017; Perdigão et al., 2017).

The ISO 9001:2015 standard establishes even more consistently the need for involvement and dedication of top management in the activities of the QMS. However, according to Sampaio et al. (2009) and Chiarini (2019), the lack of commitment and top management involvement with the QMS is one of the main obstacles organizations face during the implementation and certification of the standard.

2.3. Risk management and ISO 9001:2015

According to the ISO definitions (International Organization for Standardization, 2015, 2018), risk consists of a positive or negative effect of uncertainty in the objectives that can lead to opportunities or threats. The truth is that people who handle risks in their daily decisions and organizations face situations where they must consider and manage risks (Melo & Medeiros, 2020). However, this problem is more complex for businesses and requires the efforts of expert teams from both the strategic and operational levels, closely supported by the top management (Rybski et al., 2017; Jagodzińska, 2018). Managing risks is intrinsic to any organization that values the longevity of its business with a guarantee of the quality of its processes, products, and services; according to Tranchard (2018), risk management should be an interactive process and, in organizations, directly overseen by leadership.

The adoption of practices for risk management does not imply the establishment of specific methods, neither the adoption of ISO 31000 (Fonseca, 2015; International Organization for Standardization, 2015); although several authors, such as Sitnikov & Bocean (2015), Atan et al. (2017), Chiarini (2017) and Ezrahovich et al. (2017), present in their studies, proposals for the incorporation of risk management prescribed in the referred standard, into the context of NBR ISO 9001:2015. According to Samani et al. (2017), a reason for risk management to be integrated in other organizational process is the explicit recommendation of ISO 31000.

2.4. Implementing risk-based thinking

Since the last update of ISO 9001, research relating risks to the standard has grown considerably, especially in the period between its launch (2015) and the deadline for the transition process (2018). Crovini et al. (2021) developed an advanced, reasoned, and organized (ARO) literature review. The authors emphasize the critical

rule of entrepreneurs and companies' behavior in improving appropriate risk culture. From the articles reviewed, the authors identified as a common element that risk management in SME remains a "spot" subject, despite its importance from both an economic and social point of view, as the companies put little effort into the process of identification, assessment, and monitoring of risks.

In a systematic literature review conducted by Martins & Silva (2019, p. 261), the authors identified that most studies report the use of FMEA, "[...] probably due to its wide dissemination and customers' requirements (for example automotive and aeronautic sectors and healthcare products)". However, the tool has severe limitations, especially regarding the requirement presented in item 6.2 of the standard (International Organization for Standardization, 2015), where it requires companies to identify risks (negative aspects) and opportunities (positive aspects).

In a similar study, Rampini et al. (2019) presented the results of a literature review, which corroborates and complements the results of Martins & Silva (2019). The authors detailed publications that generally consider the use of SWOT Analysis (Strengths, Weaknesses, Opportunities, and Threats) and the model proposed by ISO 31000 as a way to meet ISO 9001:2015 in its risk-based thinking requirement. In addition, they highlighted that most of the research on the subject relates to integrated systems for quality management (ISO 9001, ISO 14001, and OHSAS 18001), aspect also discussed by Bonato & Caten (2015).

Samani et al. (2017) propose a conceptual model defined Risk Based Quality Management System (RBQMS), based on the process suggested by ISO 31000 and incorporating PDCA cycle between the steps of risk assessment and risk treatment. Despite the similarity with the model proposed in this study, RBQMS suggests a process in accordance to ISO 31000:2009 and ISO 9001:2008 requirements, both previous versions of the respective standards; besides it its main focus is the strategic level.

The choice for widespread methods, methodologies, and tools occurs through access to knowledge of such models and their application and, often, due to customer requirements - such as the use of FMEA, mandatory in the aerospace, automotive, and health industries. However, it is critical to keep in mind that the individual use of methodologies or methods such as ISO 31000:2018 and FMEA does not guarantee that the organization meets the risk-based thinking requirement. Companies should implement these methods in a collaborative and non-substitute manner to achieve the most appropriate approach for the organization (Badreddine et al., 2009; Lalonde & Boiral, 2012; Fraser & Simkins, 2016; Popa & Gulie, 2018). According to International Organization for Standardization (2018, section 4b), "[...] a structured and comprehensive approach to risk management contributes to consistent and comparable results".

Cagnin et al. (2019), conducted a research at an automotive company, identifying that they opt for a system to manage the risks associated with internal and external issues, corroborating with the abovementioned authors that suggest the use of integrated methods to incorporate risk management in accordance to ISO 9001:2015 (International Organization for Standardization, 2015).

3. Research methodology

The method performed in this study was the action research, indicated for field research where the researcher, exposed to the reality of real-time organizational change, participates in it collaboratively and interactively with the organization's members (Thiollent, 2007; Coughlan & Coghlan, 2002). Through action research, the development of the theory occurs in a cyclical process. At each stage, the researcher must learn from the experience gained with the action, investigate the process of change, have the critical sense to conceptualize what worked and what did not work, and identify the possible improvements, making the necessary adjustments and adaptations for the next cycle (Coghlan & Brannick, 2005; Zuber-Skerritt, 2018).

The adequacy check and adjustments of the model occur in each cycle of action research, supported by the analysis of internal and external specialists, and complemented by triangulation, which refers to the contrast of the theoretical foundation with the analyzed data and the observations of the researcher (Creswell & Miller, 2010). In addition, the structuring of this action research follows the concepts of Coughlan & Coghlan (2002), which characterize the method as a cyclic and interactive process of action and reflection, consisting of a pre-stage that defines the characteristics of the research and marks the beginning of the cycles, and the research cycles themselves.

3.1. Action research structuring

The conduction of this research starts in the pre-stage and goes through five research cycles (Figure 1), conducted based on the PDCA cycle, with the stages of planning, acting, analyzing, and reflecting. At the end

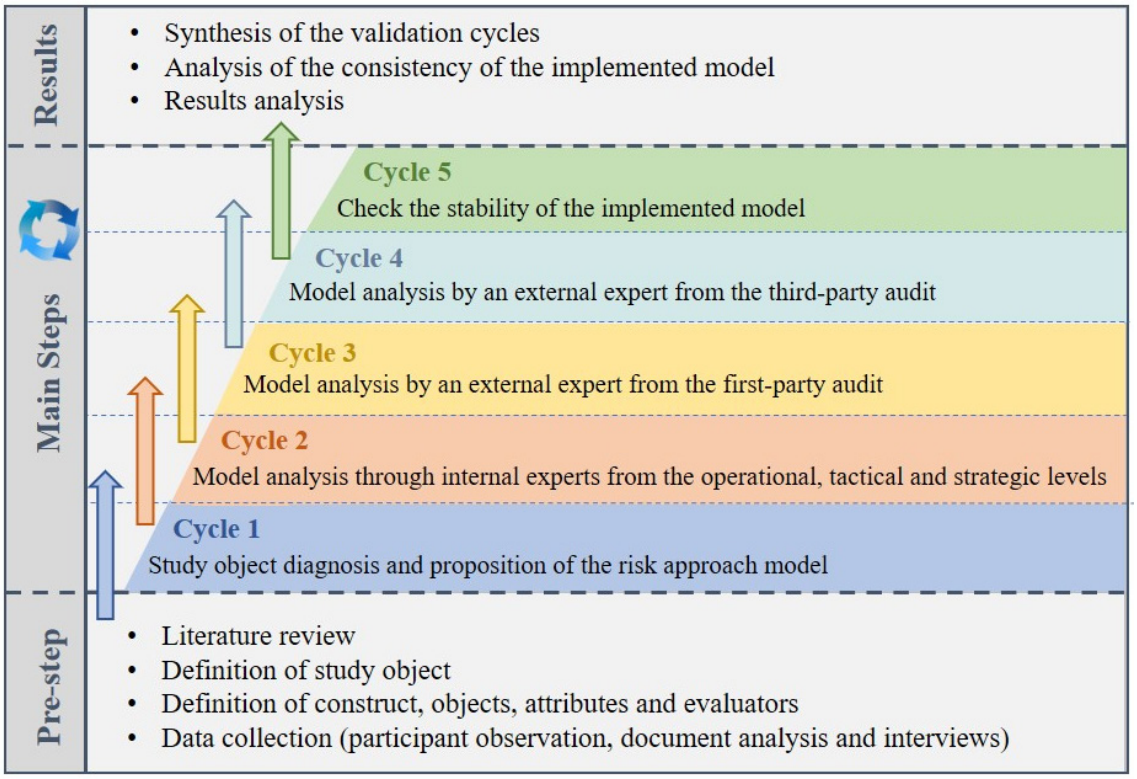


Figure 1. Synthesis of the action research process.

of each stage, necessary adjustments are proposed and implemented in a new version of the model. For this, the techniques and criteria for data collection, described in the following section, were defined.

3.1.1. Data collection techniques and criteria

The C-OAR-SE theory (Construct definition, Object classification, Attribute classification, Rater identification, Scale formation, and Enumeration and reporting), proposed by Rossiter (2002), defines the construct, object, attributes, and evaluators (Figure 2). The method is considered more global (Sarstedt et al., 2016) and allows adaptations to each research context (Rossiter, 2002). The selected objects, unfolded in their respective attributes, refer to the aspects that the evaluators must analyze to validate the construct (model) during the cycles of the action research. Figure 3 presents the attributes and details of the techniques used for data collection (Coughlan & Coghlan, 2002; Thiollent, 2007; Mello et al., 2012).

To identify the evaluators and define their participation in the cycles of action research, the authors divided two groups of specialists: internal and external. Looking to contemplate the entire company in the study, the

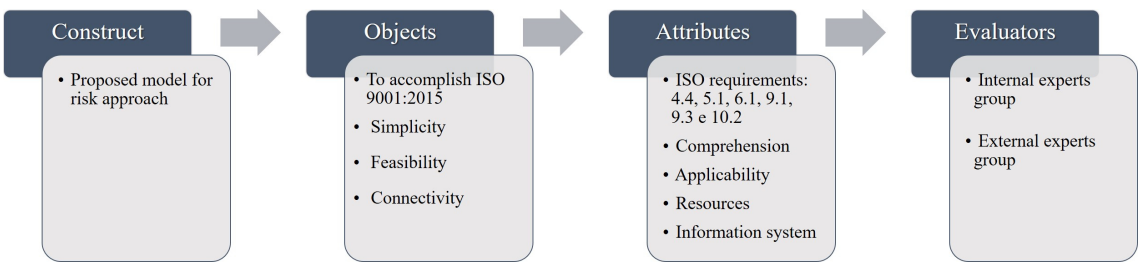


Figure 2. Definitions of research based on the C-OAR-SE theory.

authors selected, within the study object, one specialist of each subgroup, totalizing 5 experts, according to the criteria established in Figure 4. For the cycles of adequacy analysis (second, third and fourth cycles), the authors used a semi-structured interview script (Appendix A). The script followed the attributes established in Figure 3. Before its application with the groups of experts, the authors realized a pilot test with a specialist; for the last cycle, a script with open questions was developed, applied to internal specialists (Appendix B).

Construct Analysis		Data Collection		
Objects	**Attributes**	**Semi-structured interview**	**Participant observation**	**Document analysis**
To accomplish the requirements from ISO 9001:2015 related to risk-based thinking	4.4 - Quality management system and its processes (item 4.4.1 f)	X	X	X
	5.1 - Leadership and commitment (items 5.1.1 d; 5.1.2 b)	X	X	X
	6.1 - Actions to address risks and opportunities (all items in 6.1.1 and 6.1.2)	X	X	X
	9.1 - Monitoring, measurement, analysis and evaluation (item 9.1.3 e)	X	X	X
	9.3 – Management review (item 9.3.2 e)	X	X	X
	10.2 – Nonconformity and corrective action (item 10.2.1 e)	X	X	X
Simplicity in implementation and use	Comprehension	X	X	
	Applicability	X	X	
Implementation feasibility	Required resources	X	X	
Connectivity	Incorporation into the information system	X	X	

Figure 3. Objects, attributes, and techniques for data collection.

Experts		Criteria	Participation in the cycles				
			1st	2nd	3rd	4th	5th
Internal Group (3)	Top Management (strategic level)	Mandatory - To **have participated** in the ISO 9001:2015 **implementation process**; Complementary - Qualification in Quality Management/ISO 9001.	X	X			X
	Manager or process leader (tactical level)		X	X			X
	Operator, supervisor or analyst (operational level)		X	X			X
External Group (2)	First-party audit	Mandatory - **No ties** to the study object and the researcher; - Have **at least 10 years** of experience in ISO 9001; - Have participated in audits at ISO 9001:2015, as **auditor and audited**; - Have qualifications that prove their **experience**.			X		
	Third-party audit					X	

Figure 4. Criteria for selecting evaluators.

3.1.2. Pre-stage

The study object selected was an SME located in the state of Minas Gerais, Brazil. The company started in 1982, focusing on the segment of electronic systems. Using an SME as a model for conducting the research was seen as an opportunity to assist countless other organizations, both in Brazil and other countries worldwide. According to International Organization for Standardization (2016), SMEs represent a large number of national and international companies, these being extremely important for the growth and economic development of countries. Moreover, some authors, such as Crovini et al. (2021), point out that participatory and active research effectively supports scholars to spread a good business and risk culture.

The study object of this research operates in the segment of production, service and commercialization of electronic boards and other self-produced items. The company operates basically in two lines of activity, that share the same human and physical resources for its realization, which are the provision of services and the production/sale of its own products. Some of the company's products require certification by INMETRO (National Institute of Metrology, Quality and Technology), what is also seen as a means of ensuring quality.

The company was first certified by NBR ISO 9001 in the year 2003, in the version of 2000 of the standard. Since then, it has had an adequate QMS according to each update, aspect evidenced through the certificates granted by its Certification Body. During the first five years of certification, the company underwent biannual third-party audits, however, since the recertification for the 2008 version, these audits have become annual. Currently the company has the following as the scope of its QMS: "commercialization, development, assembly using SMD and PTH technologies, testing, integration and maintenance of electronic systems". Given the new requirement of NBR ISO 9001:2015, the company is faced with the following: how to implement the risk approach in the organization?

The research development occurred within the company itself, where the researchers worked with the collaborators between October 2017 and July 2019. According to needs and suggestions identified during action research, the authors performed activities such as training on the transition from ISO 9001 to the 2015 version and the main concepts, development and proposal of the initial model for risk approach, implementation and adequacy cycles, and verification of the adequacy of the model.

As part of the pre-stage, the authors based on literature reviews developed by Martins & Silva (2019) and Rampini et al. (2019), and considered the analysis of studies related to concepts and aspects of risk-based thinking in the context of ISO 9001:2015. With that analysis, the authors seek to establish the basis of the proposed model, according to researchers' suggestions, practical issues of companies, and mainly with the requirements of the standard itself. Figure 5 presents the initial proposal of the model. Together with the systematized scheme from the figure, the authors create a detailed description of each stage, delivering both for the specialists during the interviews.

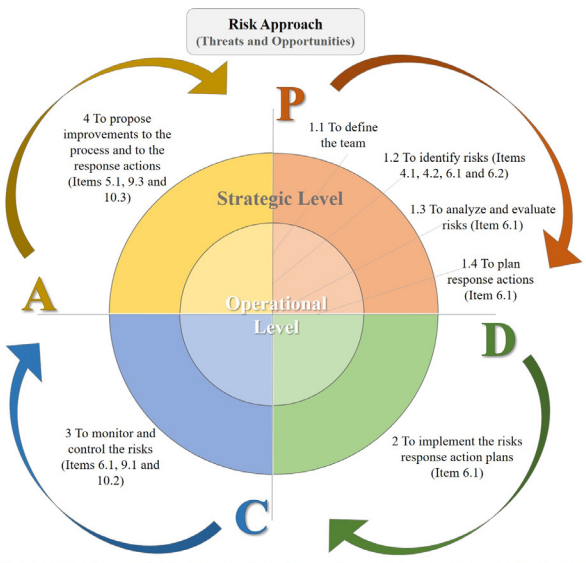


Figure 5. The initial proposal of the model for risk approach based on PDCA cycle (plan, do, check, act).

3.2. Cycle driving: implementation and adaptations of the model

3.2.1. Synthesis of cycle conduction

The research and implementation of the first version of the model occurred in a learning scenario of the ISO 9001:2015 standard. The company was at the beginning of its transition process. Over time, training, and practice, employees gained more knowledge, which provided a broader and more adequate view of the implementation of risk-based thinking. Regarding the documented information of the QMS, the company chose to keep the documentation already established for its management system, incorporating the proposed model of approaching risks in the form of procedure and quality records.

As initially presented through Figure 1, the cycles conducted during the action research were: 1) to diagnose the object of study and propose the model; 2) to analyze the model through internal experts of the three organizational levels (operational, tactical, and strategic levels); 3) to analyze the model through an internal specialist (internal audit); 4) to analyze the model through an external specialist (external audit), and 5) to verify the stability of the implemented model.

Figure 6 presents a synthesis of the cycles performed and the main results and adaptations proposed for the model. The authors already expected the completion of the first cycle without any modifications in the proposed model since the company was in the initial phase of implementing the risk management approach, in parallel to the transition process of its certification in ISO 9001.

However, from the conduction of the second cycle, through interviews with specialists from internal and external groups, it was possible to identify relevant aspects for the adequacy of the model and analyze the characteristics of the evaluators (specialists). To ensure the consistency of the changes proposed by the experts, the authors developed a more in-depth analysis of the model validation cycles (second, third and fourth cycles) and detailing the model consistency check cycle (fifth cycle).

Steps	Action research cycles				
	Cycle 1 Diagnosis and proposal	Cycle 2 Internal experts	Cycle 3 External expert	Cycle 4 Certification body expert	Cycle 5 Model consistency
1) Plan	**Period:** Oct/17 to May/18 **Objective:** proposition and implementation of the model **Method:** documentary analysis and participant observation	**Period:** May/18 **Objective:** analysis and adaptation of the model **Method:** documentary analysis, participant observation and interviews	**Period:** Jun/18, post first-party audit **Objective:** analysis and adaptation of the model **Method:** documentary analysis, participant observation and interviews	**Period:** Jul/18, post third-party audit **Objective:** analysis and adaptation of the model **Method:** documentary analysis, participant observation and interviews	**Period:** Apr/19, before maintenance audit **Objective:** check model stability **Method:** documentary analysis and interviews
2) Act	**Model:** creating procedure and records for the risks approach **Implementation** of the model at the strategic and operational levels QMS **documents** verified	**Experts:** strategic, tactical and operational levels internal experts **Interviews:** individual, according to script **Documents:** records of the implementation of the template	**Expert:** external auditor **Interview:** individual, according to script **Documents:** internal audit report	**Expert:** certification body auditor **Interview:** individual, according to roadmap and with considerations associated with the audit context **Documents:** third-party audit report	**Specialist:** internal from strategic, tactical and operational levels **Interviews:** individual, according to script **Documents:** training, critical analysis, internal audit, strategic alignment, risk analysis and changes
3) Analyze	**Results:** identification of risks and opportunities of strategic level	**Results:** similar interpretations and distinct positions **Model:** simpler for the strategic than the operational level	**Results:** the model must be operationalized **Model:** it is simple but its applicability can be complex for both levels	**Results:** commitment from employees and especially from top management is needed **Model:** complete and applicable	**Results:** identification of risks and opportunities at both strategic and operational levels **Model:** better understood and applied
4) Reflect	✓ Analyze model consistency for the operational level	✓ No distinction was identified between the model for the strategic and operational levels ✓ Everyone believes that the model contributes to ISO 9001	✓ The use of the model partially meets the requirements of ISO 9001 ✓ Internal audit report with one non-compliance and two observations	✓ The model contains the necessary items, but its effectiveness depends on each company ✓ No nonconformity or observation identified in the report	✓ Greater commitment at the tactical and strategic levels has been identified ✓ Operational level requires a "cultural" adequacy
Main changes	**No adaptations were proposed** as the model was in the early implementation phase	**Structural appropriateness** (model splitting into two drawings concerning the strategic and operational levels)	**Major and most relevant adjustments** (structure, steps, description and detail)	**Structural appropriateness** (step and text, only at the strategic level)	**No adaptation needs were identified in the model**

Figure 6. Synthesis of the implementation of the action research cycles.

3.2.2. Expert agreement analysis

The semi-structured characteristic of the interviews conducted during the verification of adequacy cycles led the authors to establish qualitative and quantitative analyses to detail the identified aspects. As can be seen in Appendix A, the interview script consists of 17 questions, eight of which are purely discursive and the other nine divided between ordinal (on a scale of one to six) and nominal (no, partially, or yes) classifications, analyzed through attribute agreement analysis, with the software Minitab® 18.

The attribute agreement analysis has as its basis the Kappa coefficient. Its performance occurs to validate the evaluations of multiple evaluators, verifying whether the respondents are consistent in their evaluations (Wynd et al., 2003). The application of the analysis is more observed in the medical area since its development happened in this context; however, there is no restriction.

The technique widely used in the literature (Zec et al., 2017) considers some assumptions for the data, such as independent units, categories of the nominal scale are independent and mutually exclusive, and impartial and independent analysis (Cohen, 1960). The existence or not of agreement, analyzed by the Kappa index value, indicates a proportion that, the closer to the unit, the stronger (or complete) is the indicated agreement (Wynd et al., 2003; Cohen, 1960). Furthermore, the software provides the parallel analysis of some statistics based on hypothesis tests.

To start the method application, the analysis of the ordinary classification questions occurred through Minitab® 18, in a separate group from those of nominal classification. However, both consider the samples from the five evaluators: 03 internal specialists (operational, tactical, and strategic levels) and 02 external specialists (internal and external audits), for which the standard defined were the external and internal audit specialists. In general, it was possible to verify that the consistency among the evaluators, given by the Kappa agreement index, is weaker than expected in both analyses. For the nominal classification questions, the Kappa coefficient was 0.25. In contrast, the binary classification index presented a coefficient of approximately 0.57, which indicates that the perception between internal experts and external experts on the subject is quite divergent.

The analyses of the discursive questions obtained from the evaluators corroborate the analysis of agreement applied to the questions of ordinal and nominal classifications. The authors noticed that the external auditor was the specialist who most closely approached the notes given by the internal auditor, defined as the standard of the analysis, with approximately 70 percent agreement. Both highlighted, during the interviews, that implementing the proposed model depends on the positioning of the organization that uses it. "[...] *the model contains everything that the standard requires; however, stating whether or not it meets the requirements is difficult because it depends on the detail and the approach used by the company. It depends entirely on the organization*"; thus, "[...] *for both strategic and operational areas, the difficulty of application will depend a lot on who is leading, if the person who is leading understands this process, is focused, and believes that it will happen, it works.*"

Internal experts, representing the three organizational levels of the object of study, had a low agreement with the standard evaluator (approximately 35 percent). The divergences identified in the analyses emphasize aspects such as the level of knowledge about risk-based thinking and ISO 9001:2015 itself, which, the higher, provides a more comprehensive and appropriate interpretation of the risk approach established by the proposed model. However, despite the quantitative analysis inconsistency, there was a convergence between the evaluators, especially regarding the need for resources to implement the proposal.

Both internal and external experts consider time as the central resource needed, aspect emphasized by the internal operational level specialist who believes that "[...] *the availability and commitment of the management and managers of the areas*" are crucial. In addition, the same specialist considers necessary training and qualification for the entire company, concerning ISO 9001:2015 and, mainly, its risk requirement. His assessment meets the external auditor's report, who considers "[...] *more important than having a systematic, disseminate the mentality of risks - train, train, train - so that everyone sees that, almost everything they do, contains a risk analysis* [...]".

Through the fifth cycle, it was evidenced that the success in the organization's risk approach depends on everyone's knowledge about the theme, their availability, and commitment, especially by the top management. The reports of internal experts support these aspects during the interviews of the last cycle. The representative of the operational level pointed out that "[...] *at the beginning of the process* [first cycle] *the team was not very engaged, perhaps because of the audit* [...] *Nevertheless, it soon came to notice a greater interest, mainly* by the Top Management." According to the tactical level specialist, there has been a significant evolution in the organization: "*I would say that we have already seen about 50 percent improvement with this procedure. The staff understood well the concepts and importance of the risk mentality.* [...] *I see thinking is changing; we are learning, even in a slow process, how to use the standard for the benefit of the company.*"

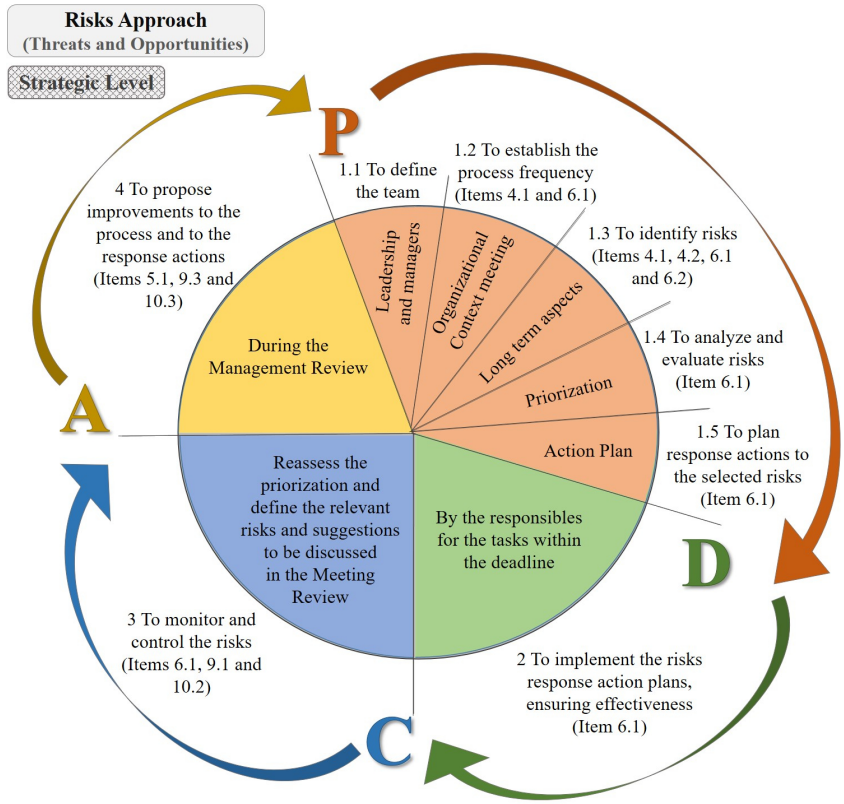
In addition, the specialists corroborate the analysis of validation cycles through the association between the need for training, commitment and availability identified, with the importance of change in organizational culture. According to the representative of the operational level, "*Risk analysis, especially by operators, requires cultural work so that they can have this in mind. Nowadays, what happens is that they end up throwing the responsibility of doing this analysis to us, from quality* [...]".

3.2.3. Final version of the proposed model

Thus, after conducting the five action research cycles, the final version of the model was defined for the risk approach. The model adequacy was verified by analyzing internal and external specialists before and after the audits performing. Finally, ensuring a period of implantation after the fourth cycle, the consistency of the model in the study object is verified with the conduction of the last cycle. Despite similar designs for strategic and operational levels, their execution is different. Maintaining them aims to emphasize the importance of the risk approach at the operational level and promote its implementation in organizations of different contexts.

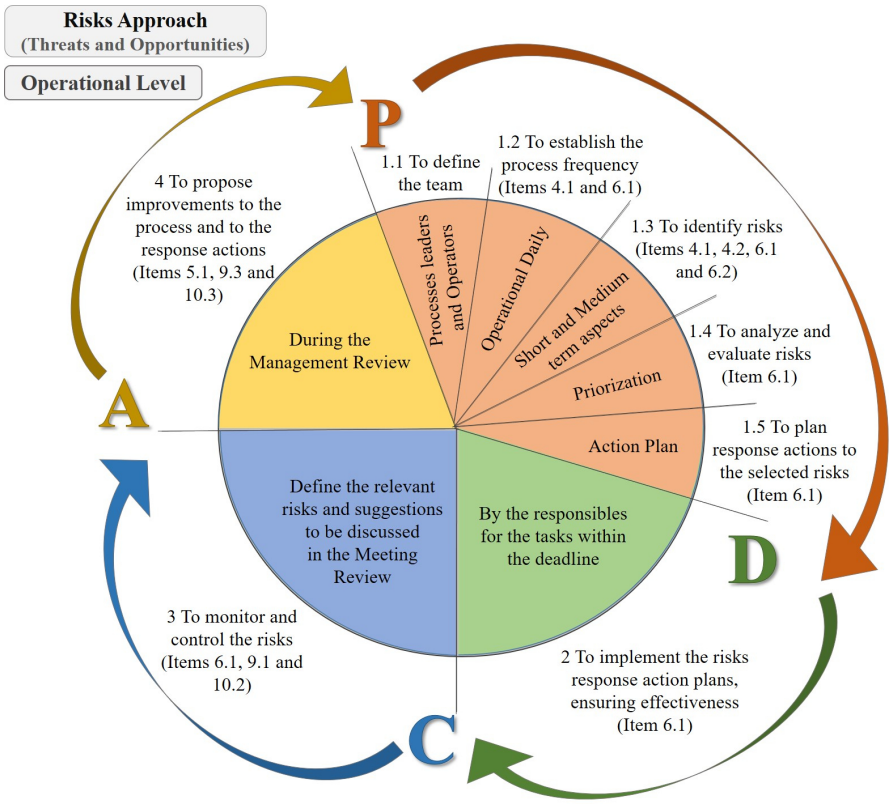
The authors suggest the implementation of the risk approach utilizing a procedure. With the systematic presented in Figures 7 and 8, it works better with a deepening of each step, emphasizing the requirements established by ISO 9001:2015, which can be prepared by each organization, following the model's steps and the concepts presented in this paper. For both strategic and operational levels, the model follows PDCA cycle, emphasizing the need for a consistent planning and also, of the analysis of the realized process, identifying improvement opportunities continuously (Rampini et al., 2019; Samani et al., 2017). This way risk management becomes part of organizational culture, as required by ISO 9001:2015. Each of the requirements directly related to RBT were carefully analyzed and are contemplated in the model.

For the strategic level it is suggested that companies define their risk management teams, with representants from leadership and managers (Vasile, 2017) departing from the organizational context analysis, where the team



[1]The items 4.1, 4.2, 4.4, 5.1, 6.1, 6.2, 6.3, 9.1, 9.3, 10.2 and 10.3 refer to ISO 9001:2015 requirements, directly related to the proposal.

Figure 7. Model for strategic level risk approach.



[1]The items 4.1, 4.2, 4.4, 5.1, 6.1, 6.2, 6.3, 9.1, 9.3, 10.2 and 10.3 refer to ISO 9001:2015 requirements, directly related to the proposal.

Figure 8. Model for operational level risk approach.

can develop the strategic planning, at the same time they analyze existing opportunities and threats that can impact organization in a long term (International Organization for Standardization, 2015; Medić et al., 2016). The process should be realized periodically, during semestral or annual meetings. To identify and analyze risks the team can use SWOT analysis, brainstorming, check lists, practical and managerial knowledge, considering as inputs the internal and external aspects, interested parties requirements, and quality objectives of the organization (Ezrahovich et al., 2017; Vasile, 2017; International Organization for Standardization, 2015; Hillson, 2002).

For the operational level there is no need for a periodical meeting. Once it is suggested that the team is formed by representants from the entire organization, especially from tactical and operational levels, it is expected that risk management will be performed in the daily activities of operations. The inputs for risks identification can be the processes change management, customers satisfaction analysis, operational improvements opportunities, first-part audits reports, along with suggestions from the operators (International Organization for Standardization, 2015; Fonseca & Domingues, 2018; Luburić, 2018). The identification and analysis can be performed with support of check lists.

The opportunities and threats evaluation can be performed with the support of probability-impact matrix and FMEA method, by prioritizing the strategic and operational risks identified. The action plans should be executed by their respective responsible and the results analyzed during the critical analysis meetings, required by ISO 9001:2015. The last phase in the Critical Analysis takes place mainly due to the participation of top management, since "[...] only top management has the information, resources, responsibility, and authority, necessary for the analysis of risks in the processes of the organization" (Vasile, 2017, p.5).

Table 1 provide a comparison between the proposal of this study and the traditional methods identified from the literature review, analysing if the requirements from ISO 9001:2015, related to RBT, are considered or not by the respective practices. Each of the mentioned requirements have specific items, as described in Appendix A; in this context, the only method that covers the requirements completely is the proposed model.

Table 1. Comparative analysis of risk management practices in the context of ISO 9001.

	ISO 9001:2015 requirements (related to risk-based thinking)					
Risk management practices	4 Organizational Context	5 Leadership	6 Planning	8 Operations	9 Performance Evaluation	10 Improvement
Proposed model	Yes	Yes	Yes	Yes	Yes	Yes
FMEA	No	No	Partially	Yes	Yes	No
ISO 31000	Partially	No	Yes	No	Yes	Yes
SWOT analysis	Partially	Yes	Yes	No	No	No

It is important to highlight that PDCA cycle was the basis for the construction of the model, in terms of planning and management activities; the specific risk management steps were structured based on ISO requirements, literature review and organizational aspects.

4. Findings and discussion

The development of this research provided an in-depth discussion on risk management in SMEs, leading to the elaboration and application of a model for risk approach in the context of ISO 9001:2015. During the cycles, it was possible to adapt the model to highlight the importance of a well-conducted risk approach, especially at the operational level. The model proposed in this research brings a comprehensive approach through which organizations can implement their processes concepts required by the ISO 9001:2015 standard inherent to risk-based thinking, contributing to its dissemination in the company's own culture. Its implementation does not require high financial investments, a scarce resource for most SMEs, although it takes time from the employees directly involved in implementing the QMS.

In addition, with the analyses of external specialists and the participant observation of the researchers, the need for organizations to give a more significant and continuous emphasis on internal training on the risk approach provided for in ISO 9001:2015 was evidenced. Especially for the operational level, if taught in a dynamic and well explanatory way, the training can contribute to the dissemination of risk-based thinking and serve as an incentive to conduct the model, especially in identifying risks and opportunities. However, as evidenced in the last cycle, the aspects inherent to the organizational culture to which employees are exposed should be considered.

The "simplicity" of the model (unfolded in understanding and applicability) depends on the level of knowledge of who uses it. Therefore, if the organization has employees with a certain level of maturity in quality management, risk management, and ISO 9001:2015, the complexity will below. A fact evidenced during the conduction of third and fourth cycles where external experts that given their vast experience suggested that the analysis of the model was evident since they did not even read the model's systematic and guide before beginning their considerations about it.

From a methodological perspective, this study represents an original contribution once its analysis and results guide a highlighted need in the literature. The model is based on literary aspects identified in articles, practical aspects obtained through their implementation, analysis, and adequacy verification in an SME, along with the requirements of ISO 9001:2015, directly and indirectly, related to risk-based thinking. Popa & Gulie (2018) were the only authors identified in the literature who developed similar research. Their model presents an adapted approach; however, it does not consider the organization's processes (item 4 of the standard) nor the definition of continuous improvement actions for risk-based thinking (item 10 of the standard). In addition, the conduction of the action research cycles of this research was essential for the practical analysis of a theoretical proposal in a real organizational context, which gives more foundation and relevance to the model (Crovini et al., 2021).

5. Research implications

The proposition of a comprehensive model allows SMEs to understand better the concepts associated with RBT while incorporating an adapted approach to their contexts, serving as guidance for SMEs in the process of implementation or adequacy of their management systems. However, it is important to highlight that the proposed model is only a means to adapt the QMS and encourage the practices of risk-based thinking in organizations. Regarding theoretical implications, the proposal of the model and its implementation contribute to the gaps in

the literature and support researchers in the future analysis of the applicability of the risk management model for SMEs from different contexts, providing consistent results and exciting discussions in the field.

6. Conclusion

The relevance of this research, especially for SMEs, evidenced through the literature review and analysis of the cycles performed, emphasizes the originality of the article and its value to organizations. Through interviews with internal and external experts and qualitative and quantitative analyses of their evaluations, the authors reaffirm that the effectiveness in understanding and implementing a risk approach is more associated with the level of knowledge that professionals have on the subject than on the model itself, corroborating the statements of Rybski et al. (2017).

The proposal of a model for risk approach makes a relevant contribution, both to the professionals of organizations and the scientific community, considering that the most widespread methods and methodologies contribute in a fragmented way to meet the requirements of ISO 9001:2015 related to risk-based thinking (Rampini et al., 2019; Martins & Silva, 2019), and considering the need to assist companies in understanding and applying the concepts related to risk management (Crovini et al., 2021), which is considered by SME, especially in the context of the standard requirements, one of the most difficult to understand and implement (Fonseca et al., 2019; Fonseca & Domingues, 2018; Rybski et al., 2017; Chiarini, 2017).

The main limitations of this research are related to the research method and the selected object of study. The action research does not generalize the results obtained (Coughlan & Coghlan, 2002), being the same guaranteed for the object of study of this investigation and, based on the literature and similar characteristics, suggested for other organizations. In addition, the agreement analysis becomes more consistent as the number of samples becomes higher; however, even with a small number of data, it was possible to reach coherent results. Although the analysis indicates there is no significant agreement between the evaluators, this does not imply the inconsistency of the model. It evidences that the higher the level of knowledge and the experience of the specialists in the ISO 9001 standard and risk management, the greater the tendency to have a strong agreement with the defined standard and, mainly, to obtain a practical implementation of the proposed risk approach.

A suggestion for future research is to apply risk-based thinking and related management models, including the proposal from this study, within the context of Quality 4.0, a present concept that emerged as the combination of quality management models and approaches with technology to promote critical competencies and features for enduring organizational success (Fonseca, Amaral & Oliveira, 2021). The authors also suggest future research to analyze the risk management practices in the medical devices sector, where the demand for controlling and monitoring the process is higher and required by specific standards (Hale et al., 2020), proposing the implementation of the risk management model.

Acknowledgments

The authors thank CNPq, CAPES, FAPEMIG and Sisvoo Sistemas Eletronicos Ltda., for support in funding.

References

Anttila, J., & Jussila, K. (2017). ISO 9001:2015: a questionable reform. What should the implementing organizations understand and do? *Total Quality Management & Business Excellence*, *28*(9-10), 1090-1105. http://dx.doi.org/10.1080/14783363.2017.1309119.

Arksey, H., & O'Malley, L. (2005). Scoping studies: towards a methodological framework. *International Journal of Social Research Methodology*, *8*(1), 19-32. http://dx.doi.org/10.1080/1364557032000119616.

Atan, H., Ramly, E. F., & Musli Mohammad, M. S. Y. (2017). A review of operational risk management decision support tool. In 7th Annual International Conference on Industrial Engineering and Operations Management (pp. 2669–2680) Rabat, Morocco.

Badreddine, A., Romdhane, T. B., & Amor, N. B. (2009). A multi-objective approach to implement an integrated management system: quality, security, environment. In *Proceedings of IEEE International Conference on Systems, Man and Cybernetics* (pp. 4728-4733). New York: IEEE. http://dx.doi.org/10.1109/ICSMC.2009.5346093.

Bonato, S. V., & Caten, C. S. T. (2015). Diagnóstico da integração dos sistemas de gestão ISO 9001, ISO 14001 e OHSAS 18001. *Production*, *25*(3), 626-640. http://dx.doi.org/10.1590/0103-6513.004811.

Cagnin, F., Oliveira, M. C., & Cauchick Miguel, P. A. (2019). Assessment of ISO 9001: 2015 implementation: focus on risk management approach requirements compliance in an automotive company. *Total Quality Management & Business Excellence*, *32*(9-10), 1147-1165. http://dx.doi.org/10.1080/14783363.2019.1677151.

Chiarini, A. (2017). Risk-based thinking according to ISO 9001:2015 standard and the risk sources European manufacturing SMEs intend to manage. *The TQM Journal*, *29*(2), 310-323. http://dx.doi.org/10.1108/TQM-04-2016-0038.

Chiarini, A. (2019). Why are manufacturing SMEs canceling their ISO 9001 certification? Research from Italy. *Production Planning and Control*, *30*(8), 639-649. http://dx.doi.org/10.1080/09537287.2019.1566840.

Cicek, H. (2018). Difficulties and solution proposals relevant in the application of ISO 9001:2015: quality management system standards to Small and Medium-Sized (SME) companies. In *Proceedings of the 8th International Conference on Information Communication and Management (ICICM '18)* (pp. 117-120). New York: Association for Computing Machinery. https://doi.org/10.1145/3268891.3268911.

Coghlan, D., & Brannick, T. (2005). Doing action in your own organization. Thousand Oaks: Sage Publications.

Cohen, J. (1960). A coefficient of agreement for nominal scales. *Educational and Psychological Measurement*, *20*(1), 37-46. http://dx.doi.org/10.1177/001316446002000104.

Cooper, H. (1998). Synthesizing research: a guide for literature reviews. Thousand Oaks: Sage Publications.

Coughlan, P., & Coghlan, D. (2002). Action research for operations management. *International Journal of Operations & Production Management*, *22*(2), 220-240. http://dx.doi.org/10.1108/01443570210417515.

Creswell, J. W., & Miller, D. L. (2010). Determining validity in qualitative inquiry. *Theory into Practice*, *39*(3), 124-130. http://dx.doi.org/10.1207/s15430421tip3903_2.

Crovini, C., Ossola, G., & Britzelmaier, B. (2021). How to reconsider risk management in SMEs? An advanced, reasoned, and organised literature review. *European Management Journal*, *39*(1), 118-134. http://dx.doi.org/10.1016/j.emj.2020.11.002.

Cusmano, L., Koreen, M., & Pissareva, L. (2018). *OECD ministerial conference on SMEs: key issues paper* (OECD SME and Entrepreneurship Papers, No. 7). Paris: OECD Publishing. https://doi.org/10.1787/90c8823c-en.

Ezrahovich, A. Y., Vladimirtsev, A. V., & Livshitz, I. I. (2017). Risk-based thinking of ISO 9001:2015 - the new methods, approaches, and tools of risk management. In *Proceedings of International Conference Quality Management, Transport, and Information Security, Information Technologies (IT&QM&IS)* (pp. 506-511). New York: IEEE. http://dx.doi.org/10.1109/ITMQIS.2017.8085872.

Fonseca, L. M. (2015). From quality gurus and TQM to ISO 9001:2015: a review of several quality Paths. *International Journal of Qualitative Research*, *9*, 167-180.

Fonseca, L. M., & Domingues, J. P. (2018). Empirical research of the ISO 9001:2015: transition process in portugal: motivations, benefits, and success factors. *Quality, Innovation. Prosperity*, *22*(2), 16-46. http://dx.doi.org/10.12776/qip.v22i2.1099.

Fonseca, L. M., Domingues, J. P., Baylina-Machado, P., & Harder, D. (2019). ISO 9001:2015 adoption: a multi-country empirical research. *Journal of Industrial Engineering and Management*, *12*(1), 27-50. http://dx.doi.org/10.3926/jiem.2745.

Fonseca, L., Amaral, A., & Oliveira, J. (2021). Quality 4.0: the EFQM 2020 model and industry 4.0 relationships and implications. *Sustainability*, *13*(6), 3107. http://dx.doi.org/10.3390/su13063107.

Fraser, J. R. S., & Simkins, B. J. (2016). The challenges of and solutions for implementing enterprise risk management. *Business Horizons*, *59*(6), 689-698. http://dx.doi.org/10.1016/j.bushor.2016.06.007.

Hale, D., Fallon, E. F., & Fitzgerald, C. (2020). An equipment qualification framework for healthcare. *IISE Transactions on Healthcare Systems Engineering*, *10*(1), 47-59. http://dx.doi.org/10.1080/24725579.2019.1671925.

Hillson, D. (2002). Extending the risk process to manage opportunities. *International Journal of Project Management*, *20*(3), 235-240. http://dx.doi.org/10.1016/S0263-7863(01)00074-6.

International Organization for Standardization – ISO. (2015). *Quality management systems requirements (ISO standard No ISO 9001:2015).* Geneva: ISO. Retrieved in 2021, April 30, from https://www.iso.org/obp/ui/#iso:std:iso:9001:ed-5:v1:en

International Organization for Standardization – ISO. (2016). *ISO 9001-2015 for small enterprises: what to do?* Geneva: ISO. Retrieved in 2021, April 30, from http://www.iso.org/publication/PUB100406.html

International Organization for Standardization – ISO. (2018). *Risk management: guidelines (ISO standard No ISO 31000:2018).* Geneva: ISO. Retrieved in 2021, April 30, from https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en

International Organization for Standardization – ISO. (2019). *Risk-based thinking in ISO 9001:2015.* Geneva: ISO. Retrieved in 2021, April 30, from https://committee.iso.org/sites/tc176sc2/home/projects/published/iso-9001-2015.html

Jagodzi□ska, N. (2018). Key changes to the ISO 9001, ISO 14001, ISO 27001 management standards in the approach to the organizational context, including risk management. *Transport Economics and Logistics*, *78*, 103-112. http://dx.doi.org/10.26881/etil.2018.78.09.

Lalonde, C., & Boiral, O. (2012). Managing risks through ISO 31000: a critical analysis. *Risk Management*, *14*(4), 272-300. http://dx.doi.org/10.1057/rm.2012.9.

Li, J., Burnham, J. F., Lemley, T., & Britton, R. M. (2010). Citation Analysis: Comparison of Web of Science®, ScopusTM, SciFinder®, and Google Scholar. *Journal of Electronic Resources in Medical Libraries*, *7*(3), 196-217. http://dx.doi.org/10.1080/15424065.2010.505518.

Luburi□, R. (2018). Creating a new model of managing change based on quality management principles and risk management principles. *Quality and Excellence*, *1-2*, 35-40.

Maron, S., Lussier, R. N., & Sonfield, M. (2019). Entrepreneurial strategy: The relationship between firm size and levels of innovation and risk in small businesses. *Journal of Small Business Strategy*, *29*(3), 33-45.

Martins, Y. S., & Silva, C. E. S. (2019). A risk management model for quality management systems based on ISO 9001:2015. In *Proceedings on 25th International Joint Conference on Industrial Engineering and Operations Management – IJCIEOM, Lecture Notes on Multidisciplinary Industrial Engineering.* Cham: Springer. https://doi.org/10.1007/978-3-030-43616-2_40.

Medi□, S., Karlovi□, B., & Cindri□, Z. (2016). New standard ISO 9001:2015 and its effect on organizations. *Interdisciplinary Description of Complex Systems*, *14*(2), 188-193. http://dx.doi.org/10.7906/indecs.14.2.8.

Mello, C. H. P., Turrioni, J. B., Xavier, A. F., & Campos, D. F. (2012). Pesquisa-ação na engenharia de produção: proposta de estruturação para sua condução. *Revista Produção*, *22*(1), 1-13. http://dx.doi.org/10.1590/S0103-65132011005000056.

Melo, F. J. C., & Medeiros, D. D. (2020). Applying interpretive structural modeling to analyze the fundamental concepts of the management excellence model guided by the risk-based thinking of ISO 9001:2015. *Human and Ecological Risk Assessment*, *27*(3), 742-772. http://dx.doi.org/10.1080/10807039.2020.1752144.

Mongeon, P., & Paul-Hus, A. (2016). The journal coverage of Web of Science and Scopus: a comparative analysis. *Scientometrics*, *106*(1), 213-228. http://dx.doi.org/10.1007/s11192-015-1765-5.

Oliveira, J. A., Nadae, J., Oliveira, O. J., & Salgado, M. H. (2011). Um estudo sobre a utilização de sistemas, programas e ferramentas da qualidade em empresas do interior de São Paulo. *Produção*, *21*(4), 708-723. http://dx.doi.org/10.1590/S0103-65132011005000044.

Perdigão, F., Jacinto, C., Lopes, S., & Matos, A. S. (2017). ISO 9001:2015 and its new requirement to address risk: a demonstration case-study. *International Journal of Systematic Innovation*, *4*(4), 46-55. http://dx.doi.org/10.6977/IJoSI.201709_4(4).0004.

Popa, F., & Gulie, N. (2018). Risk management, challenge, or good practice? *Quality - Access to Success*, *19*(166), 30-34.

Rampini, G. H. S., Berssaneti, F. T., & Saut, A. M. (2019). Insertion of risk management in quality management systems with the advent of ISO 9001:2015: descriptive and content analyzes. In *Industrial Engineering and Operations Management II. IJCIEOM 2018. Springer Proceedings in Mathematics & Statistics* (Vol. *281*). Cham: Springer. https://doi.org/10.1007/978-3-030-14973-4_20.

Rossiter, J. R. (2002). The C-OAR-SE procedure for scale development in marketing. *International Journal of Research in Marketing*, *19*(4), 305-335. http://dx.doi.org/10.1016/S0167-8116(02)00097-6.

Rybski, C., Jochem, R., & Homma, L. (2017). An empirical study on the status of preparation for ISO 9001:2015. *Total Quality Management & Business Excellence*, *28*(9-10), 1076-1089. http://dx.doi.org/10.1080/14783363.2017.1303886.

Samani, M. A., Ismail, N., Leman, Z., & Zulkifli, N. (2017). Development of a conceptual model for risk-based quality management system. *Total Quality Management & Business Excellence*, *30*(5-6), 483-498. http://dx.doi.org/10.1080/14783363.2017.1310617.

Sampaio, P., Saraiva, P., & Rodrigues, A. G. (2009). ISO 9001 certification research: questions, answers, and approaches. *International Journal of Quality & Reliability Management*, *26*(1), 38-58. http://dx.doi.org/10.1108/02656710910924161.

Sarstedt, M., Diamantopoulos, A., & Salzberger, T. (2016). Should we use single items? Better not. *Journal of Business Research*, *69*(8), 3199-3203. http://dx.doi.org/10.1016/j.jbusres.2016.02.040.

Sitnikov, C. S., & Bocean, C. G. (2015). The role of risk management in ISO 9001:2015. In Proceedings of 9th International Management Conference: Management and Innovation for Competitive Advantage. Bucharest, Romania.

Testa, J. (1998). A base de dados ISI e seu processo de seleção de revistas. *Ciência da Informação*, *27*(2), 233-235. http://dx.doi.org/10.1590/S0100-19651998000200022.

Thiollent, M. (2007). *Metodologia da pesquisa-ação*. São Paulo: Cortez.

Tranchard, S. (2018, February 15). *The new ISO 31000 keeps risk management simple*. Geneva: ISO. Retrieved in 2021, April 30, from https://www.iso.org/news/ref2263.html

Tranfield, D., Denyer, D., & Smart, P. (2003). Towards a methodology for developing evidence-informed management knowledge by means of systematic review. *British Journal of Management*, *14*(1), 207-222. http://dx.doi.org/10.1111/1467-8551.00375.

Vasile, F. (2017). A critical approach to thinking risk-based existing in the new issue of ISO 9001: 2015 standard. *EEA - Electrotehnica, Electronica, Automatica*, *65*, 19-23.

Wynd, C. A., Schmidt, B., & Schaefer, M. A. (2003). Two quantitative approaches for estimating content validity. *Western Journal of Nursing Research*, *25*(5), 508-518. http://dx.doi.org/10.1177/0193945903252998. PMid:12955968.

Zec, S., Soriani, N., Comoretto, R., & Baldi, I. (2017). High agreement and high prevalence: the paradox of Cohen's Kappa. *The Open Nursing Journal*, *11*(1), 211-218. http://dx.doi.org/10.2174/1874434601711010211. PMid:29238424.

Zimon, D. (2016). Influence of quality management systems on improving processes on small and medium-sized organizations. *Quality - Access to Success*, *17*(150), 61-64.

Zuber-Skerritt, O. (2018). An educational framework for participatory action learning and action research (PALAR). *Educational Action Research*, *26*(4), 513-532. http://dx.doi.org/10.1080/09650792.2018.1464939.

Appendix A. Semi-structured interview script for the second, third and fourth cycles

Respondent function: _____
Group: Internal experts □ External experts □
*Make available to the respondent the proposed model for risk approach and the steps detailing.

1) Explain this model for risk approach.

2) Determine the level of understanding of it:
Obvious ----------> Complex

3) Set a practical example.

4) Determine the level of applicability of the model at the strategic level:
Very easy ----------> Very difficult

5) Determine the level of applicability of the model at the operational level:
Very easy ----------> Very difficult

6) What financial resources would the organization need to carry out this model for risk approach?

7) Is it possible to incorporate this model into an organization's information system?

8) Does the model contribute to meeting the 4.1 requirement - Understanding the organization and its context of NBR ISO 9001:2015?
The organization shall determine external and internal issues that are relevant to its purpose and its strategic direction and that affect its ability to achieve the intended result(s) of its quality management system.

9) Does the model contribute to meeting the 4.2 requirement - Understanding the needs and expectations of interested parties of NBR ISO 9001:2015?
[...] the organization shall determine: b) the requirements of these interested parties that are relevant to the quality management system.

10) Does the model contribute to meeting the 4.4 requirement – Quality management system and its processes of NBR ISO 9001:2015?
Item 4.4.1) The organization shall establish, implement, maintain, and continuously improve a quality management system (point f) to address the risks and opportunities as determined by the requirements of 6.1.

11) Does the model contribute to meeting the 5.1 requirement - Leadership and commitment of NBR ISO 9001:2015?
- Item 5.1.1) Generalities, point d) promoting the process approach and risk mentality.
- Item 5.1.2) Customer focus, point b) risks and opportunities that may affect product and service compliance, and the ability to increase customer satisfaction are determined and addressed.

12) Does the model meet the requirements of item 6.1 - Actions to address risks and opportunities of NBR ISO 9001:2015?
- Item 6.1.1) (...) determine risks and opportunities for..., points a) ensure that the quality management system can achieve its intended results; b) increase desirable effects; (c) prevent or reduce undesirable effects; d) achieve improvement.
- Item 6.1.2) (...) plan, points a) actions to address these risks and opportunities; b) such as 1) integrate and implement actions in the processes of its quality management system; 2) to evaluate the effectiveness of these actions.

13) Does the model contribute to meeting the 9.1 requirement – Monitoring, measurement, analysis, and evaluation of NBR ISO 9001:2015?
- Item 9.1.3) Analysis and evaluation, point and) the effectiveness of the actions taken to address risks and opportunities.

14) Does the model contribute to meeting the 9.3 requirement – Critical analysis by the direction of NBR ISO 9001:2015?
- Item 9.3.2) Critical analysis entries by management, point e) the effectiveness of actions taken to address risks and opportunities (see 6.1).
15) Does the model contribute to meeting the 10.2 requirement – Non-compliance and corrective action of NBR ISO 9001:2015?
- Item 10.2.1) When a non-compliance occurs, including those arising from complaints, the organization shall point, e) update the risks and opportunities determined during planning if necessary.

16) Do you suggest any item to be excluded from the model? Which one(s)?

17) Do you suggest some other item to be incorporated into the model? Which one(s)?

18) Do you suggest any item from the model to be modified? Which one(s)?

19) Other comments or suggestions.

Appendix B. Interview script for the fifth cycle.

Internal experts from strategic and tactical levels – Question
How is the company using the implemented risk approach model, and what are the main results that its implementation has brought to the company?

Internal experts from operational level - Questions

1) How is the model being used by the company at its strategic and operational levels?

2) Do you see any evolution and/or improvement in the company's reality as well as its QMS with this model implementation?

3) Has there been any change in the company's commitment (at all organizational levels) to the QMS and precisely the risk-based thinking?

4) Has there been a recurrence of any problems that occurred at the beginning of the model implementation process?

5) Has there been or will soon be any auditing (internal and/or external) to verify the QMS? If so, please give details.