GESTÃO & PRODUÇÃO

ISSN 0104-530X (Print)
ISSN 1806-9649 (Online)

ORIGINAL ARTICLE

The risk mentality in organizations: an analysis of inserting risk management in ISO 9001 and ISO 14001: 2015 standards

A mentalidade de riscos nas organizações: uma análise da inserção da gestão de riscos nas normas ISO 9001 e ISO 14001:2015

Adelson Pereira do Nascimento[1,2], Washington Romão dos Santos[2], Marcos Paulo Valadares de Oliveira[2]

[1]Instituto Federal do Espírito Santo – IFES, Serra, ES, Brasil. E-mail: adelsonpn@gmail.com
[2]Universidade Federal do Espírito Santo – UFES, Vitória, ES, Brasil. E-mail: washington_romao@hotmail.com; marcos.p.oliveira@ufes.br

How to cite: Nascimento, A. P., Santos, W. R., & Oliveira, M. P. V. (2020). The risk mentality in organizations: an analysis of inserting risk management in ISO 9001 and ISO 14001: 2015 standards. *Gestão & Produção*, 27(2), e4043. https://doi.org/10.1590/0104-530X4043-20

Abstract: Risk management is related to both the external and the internal environments of organizations. Thus, the risk mentality enables the identification and minimization of negative effects, maximizing the opportunities and potential of the business. The aim of this paper is identify how the insertion of risk management requirements in ISO 9001 and 14001standards may contribute to spreading the risk mentality in organizations. We interviewed 11 auditors and consultants, with experience and training in the area, who were working in certified companies in the brazilian state of Espírito Santo. To analyze the data, the technique of content analysis was used to identify thematic categories and to relate the data to the literature. The results indicate that the certified companies have undergone a process of incorporation of risk management requirements that can be catalyzed by environmental aspects: size and nature of the company, barriers to risk management, professionalization and standardization of processes and client influence. We conclude that for companies with more complex structure, dynamic and more subject to ruptures, the integration of risk management in the business strategy represented a value, and for smaller companies in stable markets represents a cost to meet the requirements of the standard.

Keywords: ISO standards; Risk management; Content analysis.

Resumo: A gestão de riscos tem relação tanto com o ambiente externo quanto com o interno das organizações. Assim, a mentalidade de riscos habilita a identificar e minimizar os efeitos negativos, maximizando as oportunidades e potencialidades do negócio. O objetivo deste estudo é identificar como a inserção de requisitos de gestão de risco nas normas ISO 9001 e 14001 pode contribuir para difundir a mentalidade de risco nas organizações. Foram entrevistados 11 auditores e consultores, com experiência e formação na área, que estivessem atuando em empresas certificadas no estado do Espírito Santo. Para analisar os dados, foi utilizada a técnica de análise de conteúdo de modo a identificar categorias temáticas e relacionar os dados com a literatura. Os resultados apontam que as empresas certificadas passarão por um processo de

Received June 26, 2017 - Accepted Jan. 15, 2018
Financial support: None.

incorporação dos requisitos de gestão de riscos que pode ser catalisado por aspectos ambientais: tamanho e natureza da empresa, barreiras à gestão de riscos, profissionalização e padronização dos processos e influência do cliente. Conclui-se que empresas com estrutura mais complexas, de natureza dinâmica e mais sujeitas a rupturas, a integração da gestão de riscos na estratégia de negócio representava um valor, e empresas menores em mercados estáveis representa um custo para atender aos requisitos da norma.

Palavras-chave: ISO; Gestão de riscos; Análise de conteúdo.

1 Introdution

Tough competition and the turbulent environment expose each organization to unexpected situations that can disrupt its operations (Annarelli & Nonino, 2016). Therefore, the understanding of how companies can manage interruptions in operations, developing *capability*[1] (or operational capability) and becoming more prepared to face adversities is an important issue for both professionals and academics (Chung et al., 2015; Jüttner et al., 2003). Risk management is embedded in a systemic concept, related to the external and internal environment of organizations. From the point of view of the internal environment, risk management assumes a compliance perspective. In the view of the external environment, the risk is assumed from a performance perspective. Thus, the risk mentality enables an organization to identify the factors that could cause deviations in the processes and the quality management system, according to the planned results, allowing to put into practice controls that can minimize the negative effects and maximize the business opportunities (ABNT, 2015b).

Although the literature points out that quality management and environmental management are closely linked to the risk management of an organization (Arenhart et al., 2013; Nabavi et al., 2014; Srinivasu et al., 2010), it is surprising that by 2015 the standards NBR ISO 9001 (Quality Management Systems – QMS) e ISO 14001 (Environmental Management Systems – EMS) did not have mandatory requirements for linking quality management to risk management actions. Based on this shortcoming, this study examines how the new revisions to the standards published in the second half of 2015 incorporate risk-minded requirements to reorient organizations into their business operations, how they perceive and integrate those requirements with company intelligence.

Many researches on the subject aim at improving methods of identification, evaluation, mitigation and implementation of risks (Jüttner et al., 2003; Hubbard, 2009; Fahimnia et al., 2015; Taroun, 2014). Although such research has relevance, they do not investigate organizational aspects that motivate the insertion of risk management by companies and how they perceive the importance to the organization, to the point of generating value and competitive advantage (Oehmen et al., 2009; Trkman et al., 2016). While managers need tools that quickly address the decision-making process, the literature focuses on the complexity of risk assessment and the inclusion of evidence-based and firm theoretical elements.

In a first step, a detailed verification of the changes of the standards proposed by the International Organization for Standardization (ISO) was done. Then, 11 interviews were conducted with auditors of the standard, consultants and auditors of certified

[1]The term *capability* (Barney, 1999), in this article, represents the ability to be able and has the purpose of differentiating from capacity, which is commonly translated as capacity. Capability is described by Barney as the company's critical skills for managing internal and external knowledge in dynamic and risk-related processes.

companies, which operate with ISO 9001 and ISO 14001 standards. Thus, the research problem to be answered by this study is presented: **How can the insertion of risk management requirements in the ISO 9001 and ISO 14001 standards, launched at the end of 2015, contribute to spread the risk mentality in organizations**?

The work sought to evaluate the implications of this review, through the perception of the reviewers of the standard, consultants and auditors of certified companies, in order to understand how organizations have received and inserted the changes in strategy and its operations. The study is characterized as a qualitative research, collecting data through interviews and using content analysis to interpret the data. Thus, it has tried to identify gaps in the literature that deserve to be explored (Alvesson & Sandberg, 2011), among them the recent updating of standards and the need to explain how they are prepared to deal with these issues, which justifies the need to develop the topic of risk management. We chose the theoretical seam between contingency theory and resource dependence theory because we understand that they are complementary approaches that can offer an advance on the researched subject. The relationship between size and organizational structure was explained by contingency theory, in which the organizational structure varies according to the organization's strategy and its size (Donaldson, 1999). This theory evidences that the external environment establishes different requirements to the organization that by itself did influence the organizational structure. Theories of resource dependence argue that organizations are in a relationship of interdependence with the environment, so organizations change their structures and behaviors to acquire and maintain the resources needed (Pfeffer & Salancik, 1978).

In addition, to providing greater understanding of the different perceptions of companies about the risks of the business and how to develop strategies to prepare before them. Therefore, the study aimed to understand how the new revisions made to NBR ISO 9001 and NBR ISO 14001 incorporated the requirements of the risk mentality and whether these updates collaborated to reorient organizations, as well as whether they all received the same updates or if there exist differences in adoption.

Among the research findings, we emphasize that larger organizations, with greater normative requirements and exposed to greater vulnerability, are more clearly concerned with risk management, while smaller companies, belonging to more stable segments, procrastinate in inserting the management of risks as practice within the organization. Another relevant point identified was the influence of the client, that can promote the anticipated or late insertion of the risk management requirements when demanding or not the standards.

2 Theoretical background

2.1 ISO 9001 and ISO 14001

The International Organization for Standardization (ISO) originated in 1946, has its headquarters in Geneva - Switzerland - and develops international standards with the objective of inserting good practices in the organizations, making them more efficient and effective (ABNT, 2015a). The initials ISO refers to the Greek term isos, whose meaning is “equal”, and demonstrates the unifying character of the entity. The Organization has elaborated several standards, among which stand out the ISO 9001 and the ISO 14001. The ISO 9001 standard was created in 1987 to

standardize quality control standards in industries and its updates promoted changes focused on process control, customer satisfaction, continuous improvement through risk prevention and quality management. On the other hand, ISO 14001 arose from concern for environmental issues motivated by the scientific community and Stockholm Conference in 1972, which increased the pressure for the adoption of management systems that take into consideration environmental aspects. The revisions of ISO 9001 and 14001 mainly occur because they are non-technical standards that cover management issues and can be applied in any type of organization.

Regarding the focus of this research, it was observed that the only reference the previous version of ISO 9001 (ABNT, 2015b) had about the risk was in the introductory part, which mentioned (emphasis added):

> The adoption of a quality management system should be a strategic decision of an organization. The design and implementation of an organization's quality management system are influenced by: a) its organizational environment, changes in this environment and the **risks** associated with this environment (ABNT, 2015b – p. vi).

The ISO 14001 standard (ABNT, 2015c) describes only that the standard

> [...] does not include specific requirements of other management systems, such as those for quality, occupational health and safety, finance or risk management, although their elements can be aligned or integrated with those of other management systems (ABNT, 2015c – p. iv).

It is noted that, although risk management was mentioned, it was not required in the implementation and maintenance of the certification of QMS's and EMS's. This fact has therefore been an important motivator for the revision of ISO 9001: 2015 and ISO 14001: 2015 standards.

2.2 Risk management

Competition, the turbulent environment and market uncertainties expose each company to unexpected situations that may disrupt its operations (Annarelli & Nonino, 2016). Thus, the understanding of how companies can manage interruptions, risks and uncertainties, becoming more prepared to face adversities, is a topic that has been gaining attention in operations management surveys (Chung et al., 2015; Jüttner et al., 2003; Trkman et al., 2016). Risk is expressed in terms of a combination of the consequences of an event and the associated probability of occurrence of that event, that can be considered as uncertainty about the severity of the consequences of an activity or the two-dimensional combination of consequences and uncertainties (Aven, 2012). These consequences may be more or less serious, depending on the relationship between expected values, objectives or other references. ABNT (2015b, p. 4) defines risk management as the structured mapping of risks inherent to the business, containing four elements: sources, events, causes and consequences.

In risk management, in addition to the need to adapt and influence the internal and external context, the actions of those involved influence the other. Thus, the decisions taken influence the future through learning, which can generate the need to develop new skills, characterizing a complex system where organizations need to adapt to overcome difficulties (Teece & Pisano, 1994). Cost pressure influences collaboration

between firms to increase competitiveness, requiring an analytical approach to manage information and risk, and decisions to avoid, mitigate, or address them.

Supply Chain Risk Management (SCRM) involves the identification, assessment and control of internal/external risks that can affect chain performance through the coordinated and economical application of resources to minimize, monitor and control the likelihood or impact of events that may interfere in the chain as a whole (Hubbard, 2009; Jüttner et al., 2003). There are risks that can be prevented and others that must be mitigated to avoid major consequences. It should be noted that internal risks are more likely to occur, while external ones have a greater impact on the chain, since they are usually associated with events with serious consequences (Thun & Hoenig, 2011).

In this context, the supply chain risk management has been considered a critical issue for organizations, due to globalization, outsourcing, resource sharing, the need for more agile operations and the increase of terrorist threats that have contributed to the importance of SCRM (Trkman et al., 2016; Chung et al., 2015). Although organizations can adopt risk management procedures (identification, assessment, mitigation and control), and develop management skills, the ideal is to improve both.

2.3 Contingency theory

Contingency theory has emerged as an attempt to explain that there is no ideal model of structure that can be used by all organizations, contrary to the classic school of management, which emphasizes that there is a unique type of structure that could be deployed by any company, of any segment or size (Donaldson, 1999). Therefore, Woodward (1965), Burns & Stalker (1961) e Lawrence & Lorsch (1967) were the forerunners of contingency theory, demonstrating that organizational performance was affected by organizational structure, technology, and the external environment.

The relationship between size and organizational structure is explained by contingency theory and, according to theory, there is no single organizational structure model for all types of organization, but variations according to the organization's strategy and size. That is, a small organization will have a more centralized structure, while larger organizations, with greater complexity, will have more hierarchical levels and a more decentralized structure (Donaldson, 1999). Morgan (1996) characterized the contingency theory as the adaptation of the organization to the environment, evidencing that the external environment establishes different requirements to the organization that in turn influence the organizational structure. The studies of Woodward (1965) showed that there is evidence that technology played a role as important as process structure. In these studies, the output of firms differed according to the activity and the way in which they had driven growth. Where production grew in the form of large lots, the organization was more formalized and had standardized production.

2.4 Resource dependence theory

The theory of resource dependence has as its basic premise that decisions are made within organizations. Its focus is on the external environment and argues that organizations live a relationship of interdependence with the environment. For resource dependency theory, there is an organizational need to adapt to environmental needs by managing and controlling the flow of resources (Pfeffer & Salancik, 1978). Thus, it

is assumed that certain changes in the environment occur in part by the determination of the managers of the organization, when they reconcile environmental aspects with the specific interests of their organizations (Aldrich & Pfeffer, 1976). To obtain external resources that cannot be generated internally, organizations must engage in exchange relationships with other organizations in the environment, that is, organizations change their structures and behaviors to acquire and maintain the necessary resources. They strive to form mutually beneficial coalitions and capture resources that enable them to achieve satisfactory performance.

Another aspect of this perspective is that organizations try to relate to the environment and, whenever possible, try to manipulate the environment for their own benefit. A key element from the Resource Dependency perspective is the strategic choice (Chandler, 1962). In this perspective, Child (1972) notes that there are three ways in which strategic choices operate in relation to the environment. The first is based on the autonomy of the decision maker. The second is how strategic choices interact with the environment, when, for example, there is an intention to manipulate the environment or when organizations try to create demand for their products. The third way is based on how environmental conditions are perceived and evaluated differently by different people. Based on these perceptions, interpretations and evaluations it is possible to understand how the different organizations act in different ways against the same conditions.

In summary, resource dependence interprets the environment as a system of individuals and organizations that form an interrelated network. The environment influences organizational structure and individual behavior, while organizational behavior receives influences from internal factors (leadership, organizational culture, social interactions) and external factors. Each type of resource that the organization needs has a bearing, influencing the elaboration of the strategies and the way it deals with the dependence of these resources.

3 Methods

3.1 Type of research

Based on Vergara's (2009) classification, this research has a descriptive nature. Regarding the approach, this study is of a qualitative nature, being a documentary analysis, carried out in the updating of the NBR ISO 9001 and 14001: 2015 standards and semi-structured interviews with specialists who act as auditors, auditors or consultants of said standards. The perception of the auditors and consultants was chosen as a basis for analyzing the data because they experienced the changes in the organizations in which they operate and for having a comprehensive view regarding the phenomenon, size and type of organization where risk management was or not implanted.

The study, therefore, aims to analyze how the risk management requirements, inserted in ISO 9001 and ISO 14001 through the last update in 2015, have contributed to the construction of a risk mentality, that is, a more professional vision, based on the formalization, mapping and control of the risks inherent to the processes of each organization. To relate the size of the company with aspects of standardization, formalization and centralization of decision processes, the contingency theory (Donaldson, 1999) and, in a complementary way, the theory of resource dependence

(Pfeffer & Salancik, 1978) was used to analyze how environmental norms influence organizations. In order to represent the method of this approach, we have chosen to combine the steps presented by Glaser & Strauss (2006) e Corbin & Strauss (1990): data collection, coding procedures or data analysis; open coding, axial coding or concept formation and development, and selective coding or modification and integration of the concept.

3.2 Data collection

The semi-structured interviews comprised questions presented in Appendix A and were applied to the participants from September to October 2016. The questionnaire involved 10 questions about three moments of insertion of risk management requirements: before the implantation, during and afterwards as imagined that risk management will be dealt with by companies in the future. Eleven auditors and consultants were interviewed, selected by the following criteria: experience (minimum of 5 years), training in the area of study (senior level with a leading auditor training in at least one of the standards in question) and performance in companies certified in the state of Espírito Santo. The professionals interviewed are associated to Federation of Industry of Espírito Santo - FINDES, to ABNT/CB-25 – Brazilian Quality Committee[2] and to ABNT/CB-38 – Brazilian Committee for Environmental Management[3], both from the Brazilian Association of Technical Standards (ABNT).

The literature indicates that the number of participants can be from 10 to 15 if the group is homogeneous (Richardson, 1989). Therefore, in order to meet the proposed criteria, 11 interviews were carried out, being 4 auditors of ISO 9001, 1 consultant of ISO 9001, 1 auditor of ISO 14001, 1 who are both auditors and consultants of ISO 9001 (quality management) and 4 who are auditors and consultants of ISO 9001/14001 (environmental management). The interviews were conducted in person, through Skype and e-mail, and lasted from 20 minutes to 40 minutes, following the recommendations of Spradley (1979), that is, informing the objectives of the research, contextualizing on the subject and starting from semi-structured questions to introduce new questions, as the interview went through. In this way, it was possible to aggregate a large volume of information, perceptions and experiences of these professionals.

As for the experience, the interviewees have between 9 and 26 years of experience in their area of activity. Therefore, they are professionals with considerable experience and have followed the updates, in some cases collaborating to update the Brazilian version and the understandings regarding ISO 9001 and ISO 14001. In addition, they operate in different production segments, mainly in the mining, metallurgy and forestry, in large, medium and small companies, whether manufacturing or providing services.

The Table 1 describes the profile of the interviewees, the type of interview used and the distribution of the interviewees. The largest proportion of auditors and consultants in the ISO 9001 standard is related to the fact that it is related to the volume of certified companies (1.519.952 companies in more than 170 countries) in comparison to the

[2]O ABNT/CB-25 – Brazilian Quality Committee of the Brazilian Association of Technical Standards - aims to produce and disseminate the standards of Quality Management and Quality Assurance and Conformity Assessment (ABNT, 2016a).

[3]O ABNT/CB-25 – Brazilian Committee of Environmental Management of the Brazilian Association of Technical Standards aims at standardization in the field of environmental management tools and systems. Excluding test methods for pollutants, water quality, soil and acoustics; setting limit values for pollutants or effluents; setting environmental performance levels; and product standardization (ABNT, 2016b).

number of companies certified in ISO 14001 (319.324). This fact is proven by the ISO survey (ISO, 2015).

Table 1. Profile of respondents.

ID	Genre	Maximum Level of education	Function	Standard	Experience (years)		Type of interview
					9001	14001	
E1	M	Specialization	Auditor	ISO 14001	14	14	*E-mail*
E2	M	Master	Auditor e Consultant	ISO 9001 e 14001	15	15	*E-mail*
E3	F	Specialization	Auditor	ISO 9001	12	12	Presential
E4	M	Specialization	Auditor	ISO 9001	10	10	Presential
E5	F	Specialization	Auditor e Consultant	ISO 9001 e 14001	12	12	Telephone
E6	M	Specialization	Auditor e Consultant	ISO 9001 e 14001	26	21	*Skype*
E7	F	Specialization	Auditor e Consultant	ISO 9001 e 14001	10	10	Presential
E8	M	Mestrado	Auditor e Consultant	ISO 9001	11	11	*E-mail*
E9	M	Specialization	Auditor	ISO 9001	14	14	Presential
E10	M	Bachelor	Auditor	ISO 9001	9	9	Presential
E11	M	MBA	Consultant	ISO 9001	16	16	Presential

E – interviewee; M - Male; F – Female. Source: The authors.

3.3 Data analysis

In order to analyze the data collected through the interviews with specialists in the ISO 9001 and 14001 standards, the content analysis technique was used to identify thematic categories and to relate the data to the existing literature, problematizing aspects related to risk management and construction of risk-taking in brazilian companies through the insertion of new risk management.

The interviews were initially analyzed by means of a previous reading, in which the concepts and words repeated or similar that were relevant to explain the insertion of the risk management by the organizations were followed, following the recommendation of Corbin & Strauss (1990). According to these authors, coding or analysis is the procedure by which data are divided, conceptualized and related. The whole analytic process has four objectives: to build the theory, to give the scientific process the necessary methodological rigor, to help the researcher detect the biases, to develop the foundation, the density, the sensitivity and the integration necessary to generate a theory.

From there, labels were established based on the literature on risk management and on contingency theories (Donaldson, 1999) and dependence on resources (Pfeffer & Salancik, 1978) which will be used to analyze the research data, relating to the categories identified through the data processing, following the steps mentioned by Ryan & Bernard (2003). By the nature of the data, semi-structured interviews recorded and transcribed, we opted for processing through the open, axial and selective coding types. The text clippings were classified into conceptual labels for later relationship with conceptual aspects of the literature.

From a preliminary reading, we identified areas that were relevant to explain the perception of certified companies regarding risk management and how they wanted to insert those requirements into the organization. Thereafter, a second reading was carried out with the objective of labeling these passages in concepts related directly or indirectly to risk management. Thus, throughout the 11 interviews, were identified 25 conceptual labels related to organizational aspects such as formalization of processes, mapping of risks, concern with standardization of processes, visible pressures of the norm and of clients, concern with process adaptation, challenges for the implementation of risk management, performance and size of companies. The labels of all the interviews were grouped according to the repetition and relationship between them to create broader concepts that could explain the identified aspects. The next step was the creation of thematic categories from the analysis of the labels and the relationship with more comprehensive concepts. In this way, the open coding was performed, identifying six aspects: (1) size of the company, (2) barriers to risk management, (3) formalization of processes, (4) process improvement and security, influence of the institutional client and (6) organizational culture.

After the open coding, axial encoding was performed. This technique, according to Glaser & Strauss (2006) is the mean that assists the researcher to perform the integration of the categories, reducing the data and making connections between the thematic categories found through data analysis and literature (Table 2). Four categories were identified and each subdivided into two subcategories according to the relation established between them: (1) Company size and branch, related to two subcategories, large companies, and medium and small companies; (2) Barriers to risk management, subdivided in lack of a systemic view and vision based on cost; (3) Professionalization and formalization of processes, subdivided into formalization and standardization and process safety; (4) Influence of the institutional client that, through the pressure of the standard and the pressure of the clients, stimulates the adaptation of the organizational structure.

Table 2. Elements of analysis.

Categories	Perception of value	Cost Perception
Size and nature of the company	Large companies subject to vulnerability already develop risk mapping and control tools, perceived as a critical factor to the business.	They emphasize only the cost to tailor processes and operations to the requirements for risk management.
Barriers to risk management	Benefits greater than costs with the implementation and monitoring of risk management.	Tendency to visualize the costs as superior to the benefits generated by the implementation of controls, standardization and formalization of processes.
Professional and standardization of processes	Greater standardization and formalization of processes, resulting in greater knowledge about the risks of the business.	Low standardization and formalization of processes, resulting in unawareness of the risks inherent in the business.
Influence of the institutional client	Adoption of risk management to make processes safer, increase product quality, reduce waste and keep customer.	Adequacy only on paper, without major structural changes. Just to meet the standard and certification.

Source: The authors.

The next step of analysis was the selective coding, which emerges at the end of the analysis and forms the pivot or the main theme around the conceptual aspects found. The causal conditions, the context, the intervening conditions, the strategies and consequences form the theoretical relations by which the categories are interrelated, establishing some relation to explain the phenomenon researched (Corbin & Strauss, 1990). Thus, the four categories identified in the axial coding were maintained, and the category construction of the perception of value by the management demonstrated a relationship with the other categories, establishing the role of central category in the relationship, since it was identified as influencing the insertion of requirements for risk management.

4 Discussion and analysis of results

In the analysis of the interview results, we sought to relate the categories identified in the content analysis with aspects that influence the insertion of risk management in certified companies. For that, the theory of contingency was considered (Donaldson, 1999) as a theoretical lens to explain organizational behavior through organizational structures, differentiating large, medium and small companies and establishing a relationship between the branch of activity and the need for process control. In a complementary way, the resource dependency theory (Aldrich & Pfeffer, 1976; Pfeffer & Salancik, 1978) to explain how organizations adapt their structures to access important resources such as customers, markets, and credibility.

4.1 Size and branch of company activity

The size and branch of the company, considered as the size of the certified companies, is based on the organizational structure, level of centralization of decisions and complexity of the organization. Thus, larger and more risky companies, whether environmental, process or accident related, according to the nature of the activity performed, were more concerned about knowing the risks, developing ways to mitigate and prevent the occurrence of potential ruptures in processes that can cause harm and interfere in the entire production chain (Jüttner et al., 2003). As can be identified from the following report, risks in larger companies are better known:

> *In the large company the risk management was approached in light of the ISO 31.000 standard. The maintenance of risk management was developed at all hierarchical levels, being constantly analyzed in periodic meetings of critical analysis (strategic, tactical, operational risks, control measures, indicators, audits, etc.)* [...] *already developed risk management* (E5).

In medium and small companies that operate in more stable markets, the formal concern with risk management was not addressed or was not identified, as a formalized concern compared to larger companies and more exposed to risks. As the number of processes increases, it becomes more difficult to control centrally, evidencing the need to decentralize decisions, which increases the complexity of the business and insertion of risk control tools, corroborating with the contingency theory (Donaldson, 1999). In addition, small businesses do not have an integrated view of the processes and therefore are not yet ready to apply the risk management requirements.

> *In small and medium-sized companies, risk management was not addressed by companies* [...] *are not prepared for this change* [...] *In the first moment, they will basically develop the items requested only for compliance with the audits / certifications.* [...] *will need to develop in a more structured way the company's strategies, as well as its operations* (E5).

Such evidence is in line with the contingency theory, which argues that there is a difference between large, medium and small companies in adopting risk management requirements. Such differences are related to the organizational structure (Donaldson, 1999), leading to the realization that large companies perceived more clearly the benefits of developing risk management than implementation costs. The contingency theory argues that there is no single organizational structure capable of functioning indistinctly in any and every organization (Donaldson, 1999) and that the best way to manage it depends on the type of task and the environment where it is operating.

The research has shown that large companies, in areas of activity that require greater process control, already develop business risk mapping and control tools, as they identify as a critical factor of the organization the need to map processes to identify and treat risks, controlling the likelihood or impact of undesirable events in the chain (Hubbard, 2009; Jüttner et al., 2003; Thun & Hoenig, 2011), while smaller organizations of nature where risk management is not absolutely necessary perceive the updating of standards as a cost to the company, which results in reluctance to adopt criteria for formalization and development of a mentality directed to the management of business risks.

4.2 Barriers to risk management

There are numerous challenges for the implementation of risk management requirements and the creation of a risk mentality in certified organizations, among them the lack of a systemic view that makes it difficult to perceive the organization in an integrated way and the risks that involve more than one department or process. Certified companies postpone the necessary adaptations to meet the standards updates, according to the costs involved, lack of a strategic vision, and to understand that the requirements do not add value to the business, being an additional "bureaucracy" inherent in the standards. When interpreting risk management as cost, companies have difficulty inserting the requirements, as follows:

> [...] *risk management is only part of the day-to-day operations of organizations* [...] *when the organization does not perceive these requirements as cost but as value for organization, something that will add to the product or process and not just as a amount that must be paid to be certified* (E3).

This perception based on cost rather than value makes it difficult to develop a proactive approach to risk management, which allows for anticipation of disruptions, avoiding interruptions in processes and not just correcting failures after failures have already occurred, causing any interference or failure in the production or performance of the services. Thus, this perception hinders a proactive behavior to anticipate the risks (Jüttner et al., 2003). Therefore, organizations are waiting for the mandatory to implement the requirements of the standard, and should start the process in the coming years, as can be observed in the following report:

> *The main challenges for implementing risk management are the resources to start implementing* [...] *understanding risk management as a management opportunity that can help companies grow and better understand their processes, avoiding accidents, waste and increasing productivity. The* [...] *challenge is to make risk management a value of the company* [...] *part of the organizational culture* (E9).

The difficulty of aligning the strategic thinking of companies with their strategic partners in relation to risk management is another relevant factor that interferes with the implementation and control of risks. The risk mapping and control must be shared with the company's employees, because in a supply chain all are interdependent. According to the following report, among the challenges to risk management is the "[…] *difficulty of maintaining the standard when service providers change*" (E1). Thus, most certified companies have difficulty strategically perceiving the benefits of implementing risk management within processes, so as to make it inherent to day-to-day and part of strategic, tactical and operational levels planning, raising and dealing with the risks, as can be perceived in the following section:

> [...] *the majority I have observed so far has treated the subject as one more table to be inserted into the management system and delegated this analysis to a management representative, demonstrating serious leadership problems* [...] *I believe that these companies will have difficulties* [...] *most leaders are limited in their understanding and commitment to management systems* (E6).

According Guerra (2007), the proposal of the Contingency Theory is that for each set of organizational and contingent factors there will also be an adequate accounting system that, if properly adjusted, will contribute to the performance of the company. Thus, it was found that a barrier to migration to the new standards lies in the perception of the updates of the norms as costs to adjust the processes and structure of the company.

4.3 Customer influence

Larger companies exert influence over the supplier by requiring a level of conformity and quality of purchased inputs. While the standards update has a 3-year rule-making period (until 2018), companies must begin the adequacy process in the coming years, pressured by new standards requirements and customer pressure in safer processes. This influence can stimulate a critical vendor to adopt a certain level of formalization of processes that meet the requirements of that company through the pressure of a certification of a specific level of quality.

> *We do everything the norm says, because if a mill breaks, one hour represents millions and millions of dollars. So, because we are exclusive suppliers of inputs to some customers, if we do not manage risk of the production process we can generate a huge problem for the customer, and can even 'break' the customer* (E3).

The obligatoriness is a factor that will allow the insertion and formalization of risk management, however it is not the only factor that will influence the insertion as part of the "culture" of the company. The requirement of clients, which in this case are other companies, seems to have an influence in inserting the risk mentality and making these

requirements aggregate to the organizational “culture”, as can be observed in the following report: “*Some companies are adequate to the requirements of risk management, mainly due to the requirement of its customers*” (E11). Depending on the complexity of the processes and the type of company it serves, a supplier may be required to meet certain criteria. The pressure of the clients forces the adaptation of the organizational structure and the adequacy of the processes (Pfeffer & Salancik, 1978), especially when the supplier is crucial to your business because it represents a valuable resource that needs to be managed for business success.

> *Risk management requirements have always been present in the company because it is a supplier of steel for the automotive sector and this requires that it be certified [...] with this certification the company can obtain a license to negotiate internationally and expand its business, besides reducing waste, thus represents a mandatory rule, since without it does not serve its main customers* (E3).

Thus, depending on the high management understanding about the importance of mapping and controlling the risks as well as the pressure of the standard and strategic clients, the processes can be remodeled. That is, depending on the environmental contingencies, the company will adopt a more proactive or reactive stance regarding the insertion of risk management into operational processes and company planning. If risk management is perceived as an investment, it will be easier to insert requirements into the daily business, and then improve your products and processes and gain advantages (Chandler, 1962).

It is observed that the requirement of the norm obliges the companies to adopt in a first moment greater formalization of the processes and control of the risks, but, as defended by the theory of the Dependence of resources (Pfeffer & Salancik, 1978), the most important stakeholders are the customers, exerting influence when charging the company that fulfills certain quality requirements of the product or service. Large companies, especially those that are suppliers of other companies, have already adhered for some time, due to their clients' demands and because they understand that they are contingencies that can favor the maintenance of the structure and obtainment of resources that would not be possible without these guarantees. This is the case, for example, of the automotive sector, which requires a high level of conformity of parts supplied by steel companies and finishes, due to the need for safety of the final product.

4.4 Professional and standardization of processes

With regard to benefits, the concern with risk management, as well as the use of own tools to raise, analyze and control the inherent risks of each business can have advantages such as less impact in the processes in cases of ruptures and mitigation of losses. These advantages can be obtained through the standardization and formalization of the processes, however this concern is not present in most companies, especially in micro and small companies. Therefore, the insertion of risk management has made it mandatory to formalize processes and consequently the inherent risks of companies, as may be observed in the following report.

> *The reviews were valid because they enable a systemic analysis of the business, leading companies to study their risks and control measures, not just their processes. In addition to this sustainability assessment, the issue of leadership*

> *engagement reinforces the 'responsibility' of everyone to know the business / department / processes / etc. with propriety, in all instances* (E5).

Thus, the updates in the norms have brought a new requirement that can contribute to the formalization of the processes. Although companies are unfamiliar with this new perspective because they represent a new requirement that requires adjustments and investment, the insertion will depend on how the company's management understands the importance of professionalizing the processes and the company. These adaptations make companies more prepared to face adversities (Chung et al., 2015; Jüttner et al., 2003), as can be seen in the following report:

> [...] *mapping the processes, detailing each one of them, inserting quality indicators and objectives to understand what is expected of the process* [...] *helps to identify the risks and opportunities* [...] *'when a company has everything formalized it is easy to defend itself against risks, and to make the rules clearer for those who execute the actions'* (E9).

Another advantage in relation to the new requirements for risk management is the greater process safety, which is related to less rework, reduction of waste and better quality in the final product, besides allowing greater preparation to deal with situations of uncertainty and ruptures. By applying resources to minimize, monitor and control the likelihood of disruptions, the company makes its processes more secure (Hubbard, 2009).

> *When standards are compulsorily charged, organizations will have to meet the requirements* [...] *when the risks are known, it is possible to decide between the urgent, the less urgent and the non-essential, and thus to draw up measures to ensure the continuity of the processes* [...] *in addition to mapping the risks,* [...] *they must update and monitor the risks related to their processes and everything that may interfere with them* (E9).

It was identified that, for the organizations that inserted risk management, the formalization, standardization and control of the risks resulted in greater security and less rework. On the other hand, organizations that perceived only the costs of risk management presented a reactive position regarding the mapping and control of risks. They ended up avoiding expenses, adjusting the processes only when they were mandatory. This finding did not find support in any of the theoretical contributions used to verify the factors that influence the insertion of risk management in certified companies. It was noticed that all aspects were related to the construction of the perception of value by management, showing that in more complex structures, dynamic and more subject to ruptures, risk management represented a value, surpassing the vision centered only on cost. Risk management will only be part of management if it is perceived as value, allowing the delivery of better quality products.

5 Conclusion

In this research, we sought to understand the process of insertion of requirements for risk management by companies, considering a recent update in ISO 9001 and ISO 14001 standards that make these requirements a mandatory part of said standards. Based on the theory of contingency theory, which explains the differences

in organizational structure, and through resource dependence theory, which investigates the strategic choices of organizations to obtain resources. The study sought to identify the main aspects that influence organizations, which facilitate the insertion of requirements for risk management and the development of a risk mentality. Among the most relevant aspects that have arisen, the legal requirement of the norm obliges the adequacy of the processes. However, the customer's requirement is a factor that goes beyond the legal norm, because if it imposes conditions for the maintenance of the supplier, that supplier feels obligated to make the suggested adaptations to maintain its market and its customers.

The view based solely on cost may hinder the implementation of risk management or at least delay implementation, as some managers have difficulty perceiving the organization as an integrated system (systemic view). The limitation in realizing that the formalization, standardization and increase of the security of the processes can be a value can hinder the insertion of the risk management. Thus, the requirements to implement risk management as part of the business depend on the size of the business and the complexity of the business, on the influence of the customer that may or may not require greater control of business risks. In addition, there are barriers to the insertion of risk management that reside in the fact of perceiving only the costs and not as an investment that will benefit the company.

A relevant aspect of this research is the insertion of risk management as part of the company's culture, which is related to the other conceptual aspects identified and depends on many factors, the main one of which is the construction of the perception of value by management. In this way, what will determine the implantation resides in how the management of the company perceives the risk management. In other words, despite the growing concern about risk mapping and control within organizations, whether through certification or customer requirements, it will only be an integral part of the management system if it is perceived as necessary and not as a cost or mere bureaucratization of processes. Those who perceive changes in standards as cost will procrastinate their implementation, leaving it to the deadline, until it is a requirement for renewal of certifications, while those who perceive it as a value, have already begun the process of insertion or already use as part of the company.

References

Aldrich, H. E., & Pfeffer, J. (1976). *Organizations and environments*. Ithaca: New York State School of Industrial and Labor Relations, Cornell University. http://dx.doi.org/10.1146/annurev.so.02.080176.000455.

Alvesson, M., & Sandberg, J. (2011). Generation research questions through problematization. *Academy of Management Review*, 36(2), 247-271.

Annarelli, A., & Nonino, F. (2016). Strategic and operational management of organizational resilience : current state of research and future directions $. *Omega*, 62, 1-18. http://dx.doi.org/10.1016/j.omega.2015.08.004.

Arenhart, L. E., Campigotto, L., Sehnem, S., & Bernardy, R. J. (2013). adoption of sustainable practices and certification ISO 14001: a case study in a law and legal advice firm. *Revista de Gestão Ambiental e Sustentabilidade*, 2(2), 125-153. http://dx.doi.org/10.5585/geas.v2i2.55.

Associação Brasileira de Normas Técnicas – ABNT. (2015a). *NBR ISO 9000:2015: sistema de gestão da qualidade: fundamentos e vocabulário*. Rio de Janeiro: ABNT.

Associação Brasileira de Normas Técnicas – ABNT. (2015b). *NBR ISO 9001: sistema de gestão da qualidade: requisitos.* Rio de Janeiro: ABNT.

Associação Brasileira de Normas Técnicas – ABNT. (2015c). *NBR ISO 14001: sistema de gestão ambiental: requisitos*. Rio de Janeiro: ABNT.

Associação Brasileira de Normas Técnicas – ABNT. (2016a). *Sobre ABNT/CB-25*. Rio de Janeiro: ABNT. Retrieved in 2016, October 26, from http://abntcb25.com.br/sobre-abnt-cb-25/institucional/

Associação Brasileira de Normas Técnicas – ABNT. (2016b). *ABNT/CB-038: Comitê Brasileiro de Gestão Ambiental*. Rio de Janeiro: ABNT. Retrieved in 2016, October 26, from http://www.abnt.org.br/cb-38

Aven, T. (2012). The risk concept-historical and recent development trends. *Reliability Engineering & System Safety*, 99(951), 33-44. http://dx.doi.org/10.1016/j.ress.2011.11.006.

Barney, J. B. (1999). How a firm's capabilities affect boundary decisions. *Sloan Management Review*, 40(3), 137.

Burns, T., & Stalker, G. M. (1961). *The management of innovations*. London: Tavistock.

Chandler, A. D. (1962). *Strategy and structure: chapters in the history of the american industrial enterprise*. Cambridge: Massachusetts Institute of Technology Press.

Child, J. (1972). Organization structure, environment and performance. *Sociology*, 6(1), 12-27. http://dx.doi.org/10.1177/003803857200600101.

Chung, S. H., Tse, Y. K., & Choi, T. M. (2015). Managing disruption risk in express logistics via proactive planning. *Industrial Management & Data Systems*, 115(8), 1481-1509. http://dx.doi.org/10.1108/IMDS-04-2015-0155.

Corbin, J. M., & Strauss, A. (1990). Grounded theory research: procedures, canons, and evaluative criteria. *Qualitative Sociology*, 13(1), 3-21. http://dx.doi.org/10.1007/BF00988593.

Donaldson, L. (1999). Teoria da contingência estrutural. In S. R. Clegg, C. Hardy & W. R., Nord (Eds.), *Handbook de estudos organizacionais: modelos de análise e novas questões em estudos organizacionais* (M. Amatucci, Trad., p. 105-133). São Paulo: Atlas.

Fahimnia, B., Tang, C. S., Davarzani, H., & Sarkis, J. (2015). Quantitative models for managing supply chain risks: a review. *European Journal of Operational Research*, 247(1), 1-15. http://dx.doi.org/10.1016/j.ejor.2015.04.034.

Glaser, B. G., & Strauss, A. L. (2006). *The discovery of grounded theory: strategies for qualitative research*. New Brunswick: Aldine Transaction.

Guerra, A. R. (2007). *Arranjos entre fatores situacionais e sistema de contabilidade gerencial sob a ótica da teoria da contingência* (Dissertação de mestrado). Universidade de São Paulo, São Paulo.

Hubbard, D. (2009). *The failure of risk management: why it's broken and how to fix it*. Hoboken: John Wiley & Sons.

International Organization for Standardization – ISO. (2015). *The ISO survey 2015*. Genebra: ISO. Retrieved in 2016, October 26, from http://www.iso.org/iso/the_iso_survey_of_management_system_standard_certifications_2015.pdf

Jüttner, U., Christopher, M., & Peck, H. (2003). Supply chain risk management outlining an agenda for future research. *International Journal of Logistics Management*, 6(4), 97-210.

Lawrence, P. R., & Lorsch, J. W. (1967). *Organization and environment: managing differentiation and integration*. Boston: Harvard University Press.

Morgan, G. (1996). *Imagens da organização* (C. W. Bergamini & R. Coda, Trad.). São Paulo: Atlas.

Nabavi, V., Azizi, M., & Faezipour, M. (2014). Implementation of quality management system based on ISO9001:2008 and its effects on customer satisfaction. *International Journal of Quality & Reliability Management*, 31(8), 921-937. http://dx.doi.org/10.1108/IJQRM-04-2013-0064.

Oehmen, J., Ziegenbein, A., Alard, R., & Schönsleben, P. (2009). System-oriented supply chain risk management. *Production Planning & Control: The Management of Operations*, 20(4), 343-361. http://dx.doi.org/10.1080/09537280902843789.

Pfeffer, J., & Salancik, G. R. (1978). *The external control of organizations: a resource dependence perspective*. Stanford: Stanford University Press.

Richardson, R. J. (1989). *Pesquisa social: métodos e técnicas*. São Paulo: Atlas.

Ryan, G. W., & Bernard, R. (2003). Techniques to identify themes. *Field Methods*, 1(15), 85-109. http://dx.doi.org/10.1177/1525822X02239569.

Spradley, J. P. (1979). *The ethnographic interview*. Belmont: Wadsworth Group & Thomson Learning.

Srinivasu, R., Reddy, G. S., Sreenivasarao, V., & Rikkula, S. R. (2010). The contributions of TQM and six sigma in the organizations to achieve the success in terms of quality. *International Journal of Computers and Applications*, 8(4), 16-22. http://dx.doi.org/10.5120/1200-1704.

Taroun, A. (2014). Towards a better modelling and assessment of construction risk: insights from a literature review. *International Journal of Project Management*, 32(1), 101-115. http://dx.doi.org/10.1016/j.ijproman.2013.03.004.

Teece, D., & Pisano, G. (1994). The dynamic capabilities of firms: an introduction. *Industrial and Corporate Change*, 3(3), 537-556. http://dx.doi.org/10.1093/icc/3.3.537-a.

Thun, J., & Hoenig, D. (2011). An empirical analysis of supply chain risk management in the German automotive industry. *International Journal of Production Economics*, 131(1), 242-249. http://dx.doi.org/10.1016/j.ijpe.2009.10.010.

Trkman, P., Oliveira, M. P. V., & McCormack, K. (2016). Value-oriented supply chain risk management: you get what you expect. *Industrial Management & Data Systems*, 116(5), 1061-1083. http://dx.doi.org/10.1108/IMDS-09-2015-0368.

Vergara, S. C. (2009). *Projetos e relatórios de pesquisa em administração* (10. ed.). São Paulo: Atlas.

Woodward, J. (1965). *Industrial organization: theory and practice*. New York: Oxford University Press.

Appendix A. Interview script.

I- INTERVIEWER IDENTIFICATION

1. Full name:

2. Education (graduation / maximum degree):

3. Experience:

a) **Works with which Management System**: ( ) ISO 9001 ( ) ISO 14001

b) **What is your experience with the above standard** (s): ( ) Consultant ( ) Auditor

c) **How much time (years / months) work with certification of companies in the norm (s) cited above**:

d) **Sector of activity**:

II- ABOUT RISK MANAGEMENT (There is no word limit for response)

1. Have you participated in review committees for the standard (s)? What were your contribution?

2. How was risk management addressed in the organizations it operates prior to the standard updates?

3. How do you evaluate the updates to the ISO 9001 and ISO 14001 standards related to risk management that were inserted at the end of 2015?

4. How do you evaluate risk management in certified companies? Do you believe they are prepared to fully meet the new requirements of ISO 9001 and ISO 14001?

5. How have organizations received and introduced changes related to risk management, strategy and operations?

6. How do you evaluate the requirements for certifying a company in accordance with ISO 9001 and ISO 14001, specifically considering risk management?

7. Do you have any suggestions for improvement in the implementation of risk management by companies that have initiated the process recently or have not yet implemented?

8. What are the main challenges to efficiently implement risk management in organizations? Because?

9. What is the impact of the insertion of risk on the said standard (s) for the organizations in which it operates?

10. Would you like to make any additional comments on the subject?

GESTÃO & PRODUÇÃO

ISSN 0104-530X (Print)
ISSN 1806-9649 (Online)

ERRATUM

Erratum

In the article “The risk mentality in organizations: an analysis of inserting risk management in ISO 9001 and ISO 14001: 2015 standards”, DOI number https://doi.org/10.1590/0104-530X4043-20, published in the journal *Gestão & Produção*, vol. 27, no. 2, e4043, 2020, on page 1, in the article translated title:

Where it reads:

A mentalidade de riscos nas organizações: uma análise da inserção da gestão de riscos nas normas ISO 9001 e ISSO 14001:2015

It should be read:

A mentalidade de riscos nas organizações: uma análise da inserção da gestão de riscos nas normas ISO 9001 e ISO 14001:2015