Similarities and differences between COSO ERM and ISO 31000 – descriptive and content analyzes

Gabriel Henrique Silva Rampini (Universidade de São Paulo)

gabrielrampini@usp.br

Fernando Tobal Berssaneti (Universidade de São Paulo)

fernando.berssaneti@usp.br

The academic interest on risk management research increased over the last years. What was previously treated in isolation, these days are essential to be treated by the entire company. Thus, the parts that make up the risk processes of the organizations must be studied in a continuous way aiming at optimizing the whole process. Despite having several guidelines, COSO ERM and ISO 31000 are the most accepted by risk management professionals. Therefore, the present article aims to outline a profile on COSO ERM and ISO 31000 into the scientific productions and highlight the main similarities and differences between them. In order to reach the objective, a descriptive and a content analysis was carried out, with samples of documents extracted from the Web of Science Core Collection database, from 2017 to 2021. After the analyzes, it was possible to identify the consistent evolution of the publications, diversity of journals interested in the subject, interdisciplinarity between quality management and risk management and finally list differences and similarities between COSO ERM and ISO 31000.

Keywords: risk management; ISO 31000; COSO ERM; bibliometric analyses

1. Introduction

The decision-making process involves risk, which can appear as a threat to planning or an unplanned opportunity (OLECHOWSKI et al., 2016). Thus, there is a need to carry out risk management, which aims to increase the probability of success in the complex, multidisciplinary and challenging activity of managing projects and developing products (OLIVA, 2016). Thus, it is indispensable to any business environment, as the risk affects the results of the processes and is fundamental to guarantee the achievement of strategic objectives (THOMYA; SAENCHAIYATHON, 2015).

Within this reality, it is possible to identify structures that enable the implementation and development of risk management activities in institutions (MUZAIMI; CHEW; HAMID, 2017). Two structures spread among organizations are COSO ERM and ISO 31000 (DIAS, 2017). From this perspective, it is highlighted that the theme is explored both in the academic literature (by researchers seeking scientific support for recent methodologies), and in the corporate world (by entrepreneurs seeking competitive advantage from their companies in relation to competitors) (KARANJA, 2017; PREWETT; TERRY, 2018).

Due to the recent edits made to both COSO ERM in 2017 and ISO 31000 in 2018, a comparison between the two is necessary so that risk managers have the exact idea of what to expect from the framework and use it in the best possible way in the implementation of risk management processes in their organizations (CROVINI; SANTORO; OSSOLA, 2020).

Although risk management is seen as the most efficient way to reach the strategic objectives of the institutions (ANNAMALAH et al., 2018), further studies are needed to compare these two frameworks (GOVENDER, 2019; PREWETT; TERRY, 2018).

Therefore, there is an important gap not addressed in the literature on the comparison between COSO ERM and ISO 31000, and both academia and industry can benefit from this debate. In order to adress such research gap, we review, analyze and outlined a profile of the existing academic research regarding COSO ERM and ISO 31000, highlighting the main similarities and differences of these two frameworks.

The present article was structured in four further sections to better address the current research goal. In the following section, a theoretical framework is presented to introduce the main definitions and outline the current debate regarding the researched topic. Section 3 describes the methods used to search, collect, analyze and synthesize the data collected. Section 4 presents the results of the bibliometric analysis conducted and discusses the main findings uncovered by

it during the analysis. Finally, Section 5 presents some conclusions, implications, limitations of this article and some suggestions for further research.

2. Theoretical Framework

2.1. Risk Management

Risk management is the integration of the organizational culture and available resources with the strategy and execution used by organizations, to manage risks in the creation, preservation and obtaining of value (COSO, 2017). It should be noted that the evolution of this concept is the result of the experience obtained by institutions after financial crises, management of uncertainties and regulatory actions combined with academic research on the subject (PATÉ-CORNELL; COX, 2014).

During the 1970s, the literature established the academic bases for risk management activities. The article "The risk management revolution" published by Felix Kloman in Fortune magazine in July 1976, made risk management famous as a corporate trend, being one of the first texts to establish the relationship between the top management of organizations and the functions related to the business risk management.

Since then and to the present day, the permanent relationship between risk management and company objectives has made the process a key factor in organizations (ANDRADE ABREU; ZOTES; FERREIRA, 2018). This role also arises from the perception that risks must be managed in an integrated manner, focusing on the company's strategy. In this perspective, Chakraborty et al. (2019) states that the main drivers of risk management are corporate governance requirements and regulatory pressures, coupled with the demand from administrators and investors for a greater understanding of strategic and operational risks.

It should be noted that risk management is not intended to completely eliminate an organization's business risks. In order for the possible impacts to be minimized, the process must focus on identifying, measuring and controlling the risks (SAEIDI et al., 2019). Thus, risk management is an important tool for managers to make the most appropriate decisions in their companies, which is why organizations adopt policies aimed at implementing a specific risk function (Olechowski et al., 2016).

According to Aven and Zio (2014), for the reason that risk management is increasingly part of the culture of institutions, the techniques of evaluation and management have matured through research and application of results. New technologies and conceptual structures are emerging. Companies that do not adopt the best market practices and do not respect the imposed

regulations will be susceptible to irreparable damage to reputation, competitiveness and market value (Safa, Von Solms, and Furnell, 2016).

It is emphasized that the approaches and methods regarding the risk management process are supported by established guidelines and standards. The two most usual and internationally recognized models are ISO 31000, whose most recent version was published in 2018 and COSO ERM, which was last updated in 2017 (GOVENDER, 2019; PREWETT; TERRY, 2018).

2.2. COSO ERM

In 1985, the National Commission on Fraudulent Financial Reporting, popularly known as the "Treadway Commission", was created in the United States, in reference to the surname of its president, lawyer James Treadway Junior. The commission's objective was to carry out studies regarding the financial and accounting frauds that occurred on North American soil (Vanasco, 1999).

In the early 1990s, after the success of the work carried out by the “Treadway Commission”, its representatives decided to expand the work and transformed it into a committee, the Committee of Sponsoring Organizations of the Treadway Commission (COSO). Since then, the committee's objective has been to develop comprehensive structures and guidelines on internal control, corporate risk management and fraud prevention, designed to improve performance and organizational oversight and reduce fraudulent actions in organizations (COSO, 2017).

The first model presented by the committee was the COSO Internal Control - Integrated Framework structure, in 1992, known as COSO 1 and which dealt with procedures related to internal controls. However, it was only in 2004 that a specific model for risk management was presented, the COSO Enterprise Risk Management - Integrated Framework (WILLIAMSON, 2007). Despite being known as COSO 2, the structure aimed at risk management is not a new edition of COSO 1 (Internal Controls). In reality, they are complementary structures. So much so that the last update of the so-called COSO 1 occurred in 2013 and that of COSO 2 in 2017.

According COSO (2017), the structure highlights the need to consider the risks in the process of defining the strategy and in evaluating performance, and the integration of these two areas is essential. The risk management process is an integrated system of strategic planning, continuous monitoring, learning and improving organizational performance. COSO ERM highlights the importance of having a definition of strategic objectives aligned with the organization's mission, vision and values in order to strengthen its performance (ABDUL RAHMAN; AL-DHAIMESH, 2018).

Finally, it is emphasized that companies, in order to carry out risk management according to the components and principles established by COSO ERM, must learn to deal with the proliferation and volume of data, understand the impact caused by new technologies and manage the cost versus benefit ratio of corporate governance processes (COSO, 2017).

2.3. ISO 31000

The first edition of the ISO 31000 Risk Management - Guidelines was published by the International Organization for Standardization (ISO) in 2009. It is a structure that standardizes risk management, through its methodology, concepts and terminologies. Although, to date, the standard is not certifiable, there has been a notable acceptance in the corporate world (Purdy, 2010). It is also noteworthy that it is a standard that covers all types of organizations, and is not directed to a specific sector (ISO, 2018).

Due to its popularity and the natural evolution of research on the subject, in February 2018, a new version of ISO 31000 was presented. The current version presents a more comprehensive and strategic view to managers, detailing the principles and methodologies used in management of risks (RAMPINI; TAKYIA; BERSSANETI, 2019).

According to ISO (2018), the methodology focuses on establishing strategies, achieving goals and making informed decisions. Therefore, risk management must be part of corporate governance, be an interactive process and consider the organization's internal and external contexts (GOVENDER, 2019). The scope of the model aims to create and protect the institution's value. In order for risk management to be efficient, effective and consistent, ISO 31000 directs the organization to be based on three fundamental pillars: the principles, the structure and the process (SUYASA; LEGOWO, 2019).

The development of the proposed structure encompasses integration, design, implementation, evaluation and ultimately the improvement of the risk management process, thus supporting the institution in governance and significant activities (ISO, 2018). This structure allows current practices to be assessed and any gaps, which prevent the optimization of risk management, to be filled (BJÖRNSDÓTTIR et al., 2021).

In practice, it is an iterative process, which can be applied at the strategic, operational, program or project levels. It is also emphasized that the process must adapt to the particularities of each organization, so that in fact it adds value, advises the manager in decision-making and assists in achieving the previously planned strategic objectives (ISO, 2018).

3. Methods

In order to achieve the objective of the present study, the research methodology used is bibliometrics. It refers to a technique that aims to obtain an objective understanding of the literature on a given topic. It begins with a literature review, consisting of three distinct phases (planning, review and results) and then a descriptive analysis in the presentation of the results.

3.1. Planning

The planning phase begins with the proposal to identify how the COSO ERM and ISO 31000 frameworks are inserted in the scientific productions on risk management. We chose to use the Web of Science Core Collection due to the fact that it has a collection that covers the most cited publications in the literature, access to full-text articles and the complete extraction of the data necessary for the analyzes carried out during the research.

In the search platform, the following filter criteria were inserted: articles as the type of document, as they represent the trend of study in the areas of knowledge more quickly; the period starting in 2017 and ending in 2021, in order to have a view of the scientific productions after the risk management frameworks have been updated and finally the research fields that encompass essential items in the selection of articles, such as title, abstract and author keywords.

The general structure of the search strings has two main identifiers: one from COSO ERM and one from ISO 31000. Thus, in order to map the literature with greater robustness, the union used in the searches is presented: "*COSO ERM*" OR "*ISO 31000*".

3.2. Review

The review phase began with the first results obtained through the search carried out in the database. Initially, the database presented 97 articles.

Then, the titles and abstracts of all articles were analyzed. Those that did not directly address any of the search strings were eliminated, as they would not help in the execution of the objective proposed by this study, such as articles that addressed risks in surgical procedures and risks of environmental disasters. Thus, 82 articles made up the sample used to prepare the descriptive analyses.

3.3. Results

A descriptive analysis was conducted with the 82 articles in the dataset to identify the most relevant journals, the total publication per year during the timespan selected, main institutions that published on the topic and main keywords used.

Regarding the most cited journal, the *Quality Access to Success* was the main source of documents addressing the topic discussed in this document, with a total of 5 published articles. This is a widespread theme among the various types of publications, since the 82 articles are published in 65 different sources. Table 1 highlights information about the journals that published at least 2 articles of the selected sample, thus serving as reference for researches.

Table 1. Journal Information

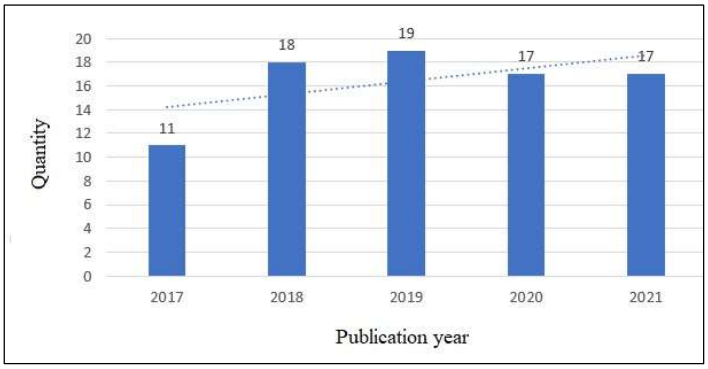
Journal	SJR (2020)	Quantity
Quality Access to Success	0.21	5
Sustainability	0.23	5
Computer Standards Interfaces	0.56	3
3C Empresa	-	2
Journal of Cleaner Production	1.94	2
Journal of Emerging Technologies in Accounting	0.76	2
Journal of Environmental Management	1.44	2
Reliability Engineering System Safety	1.76	2
Revista Inclusiones	-	2
Total Quality Management Business Excellence	0.73	2

Source: The authors

The number of documents published between January 2017 and December 2021 is illustrated in Figure 1, allowing to identify an expected trend towards an increasing volume of academic documents regarding COSO ERM and ISO 31000 as an integral part of risk management.

It is possible to note that from 2018 to 2021 the number of annual publications remained practically constant, demonstrating solid research on the subject in the literature.

Figure 1. Distribution of documents published between 2017 and 2021



Source: The authors

Regarding main institutions, Table 2 presents the universities that published at least 3 articles during timespan considered in the sample. It is worth mentioning the Federal Fluminense University, a Brazilian institution with 5 publications and the countries Spain and Belgium with 2 institutions highlighted, demonstrating that risk management has been discussed in various academic communities around the world.

Table 2. Institutions that most published

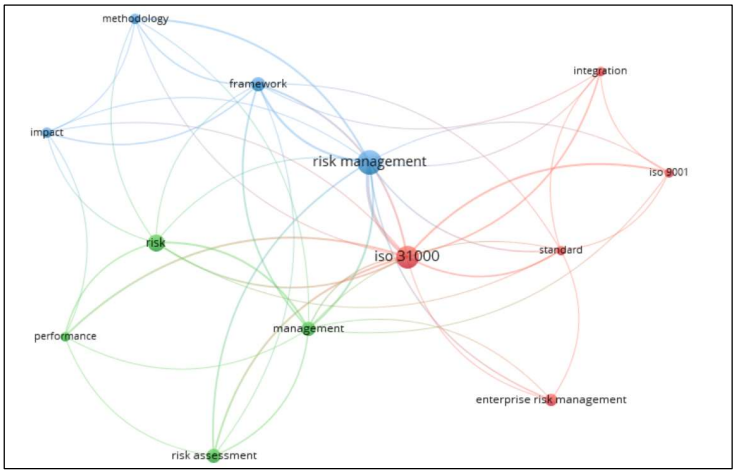
Affiliation	Country	Quantity
Federal Fluminense University	Brazil	5
Polytechnic University of Valencia	Spain	3
University of the Balearic Islands	Spain	3
Delft University of Technology	Netherlands	3
Katholieke Universiteit Leuven	Belgium	3
University of Antwerp	Belgium	3
Luxembourg Institute of Science and Technology	Luxembourg	3

Source: The authors

The VOSviewer® software was used to analyze the keyword network of the sample (Figure 2). As a result of the search strings used, it is possible to prove the relationship between the themes of risk management and their frameworks in the selected sample.

In addition, the term ISO 9001 should be highlighted. Although the term was isolated in the search strings, a relevant occurrence of this word was verified, thus demonstrating that it is an area directly related to scientific research that deals with risk management.

Figure 2. Keywords network



Source: The authors

4. Findings

Based on the descriptive analysis performed and analyzing all the articles in the sample, it is also possible to perform a content analysis about the risk management structures.

Content analysis is a technique of textual analysis through the codification of information, aiming to analyze the content of documents in a systematic, objective and reliableway. Therefore, the analysis developed in this article illustrated similarities and differences between COSO ERM and ISO 31000, according theses applications in risk management processes.

Regarding the similarities, it is verified that both structures encourage the implementation of risk management processes in organizations (SOUZA et al., 2020), they are not subject to certification by certifying companies (DIAS, 2017), they are aligned with the current market due to recent editions (MARTINS et al., 2018) and require the support of Top Management for having a top-down approach (TORREGROSA; SOLER; PEREZ-BERNABEU, 2019).

The fact that the two frameworks present mechanisms for the implementation and monitoring of the risk management process makes the topic recurrent in organizations and makes it possible to identify how the tool adds value to the organizations' strategic objectives.

Although both are not certifiable standards, they have a high degree of credibility on the part of stakeholders, since they are a competitive differentiator between companies and their competitors and, due to recent updates, they are aligned with the best practices related to business management. In this way, the organization that does not adopt one of the two structures to implement the risk management process is at a disadvantage in relation to the others in the sector.

Having concluded the similar aspects, it should be noted that both frameworks require direct support from Top Management in order for them to be implemented. As foreseen in the structures, although risk management has capillarity throughout the organization, it is inserted in a top-down context, in which COSO ERM and ISO 31000 are planned from the top to the bottom of the organization.

Regarding the differences, it is verified that ISO 31000 is direct and objective (BOLANOS et al., 2019) and COSO ERM has a long-winded character (DIAS, 2017). On the other hand, ISO 31000 emphasizes theoretical aspects of risk management (AVEN; YLONEN, 2019); COSO ERM emphasizes the practical aspects (CALLAHAN; SOILEAU, 2017). COSO ERM's focus on risk factors (KARANJA, 2017; ROD et al., 2020) and the ease of ISO 31000 integration with ERP systems (BARAFORT; MESQUIDA; MAS, 2017) are the last two differences identified in this study.

Because it follows the ISO standard, ISO 31000 has a more manager-friendly language when compared to COSO ERM, which follows a more independent structure. In this way, ISO 31000 is considered objective, while COSO ERM has a rule considered verbose.

It is possible to identify that COSO ERM has a practical bias, while ISO 31000 has a theoretical focus. Thus, while ISO 31000 has great potential in planning matters, the COSO ERM differential is in the execution of risk management activities.

COSO ERM places greater emphasis on the identification and treatment of risks, while ISO 31000 emphasizes meeting the strategic objectives of organizations, that is, while the former is focused on risk factors, avoiding their consequences; the second is centered on the governance aspects of the organization.

Concluding the differences between the structures, it is worth highlighting the alignment of ISO 31000 with the main ERP systems, since they use ISO standards as a reference. The integration between COSO ERM with ERP systems demands greater complexity of integration with management softwares.

5. Conclusion

In order to address the literature gap concerning similarities and differences between COSO ERM and ISO 31000, the present research aimed to review, analyze and outline a profile of the existing academic research regarding these two risk management frameworks.

A bibliometric analysis composed of a descriptive and content analysis was used as method to address the research aim. Articles were extracted from the Web of Science Core Collection database. The final sample that served as the basis for the descriptive and content analysis was composed of 82 articles published between 2017 and 2021.

In the first part of this research, a descriptive analysis was carried out to obtain an overview about COSO ERM and ISO 31000 in the literature. It has been found that the subject is widespread in 65 academic journals, showing that there are fields for research and publications. It is possible to note that from 2018 to 2021 the number of annual publications remained practically constant, demonstrating solid research on the subject in the literature.

Led by universities in Brazil, Spain and Belgium, another relevant aspect was the number of different institutions that published about the theme, demonstrating that risk management has been discussed in various academic communities around the world. Analyzing the keywords, a relevant occurrence of *ISO 9001* was verified, thus demonstrating that it is an area directly related to scientific research that deals with risk management.

When categorizing the studies, similarities and differences became evident regarding risk management and its application according COSO ERM and ISO 31000. Regarding the similarities, it was verified that both structures encourage the implementation of risk management processes in organizations, they are not subject to certification by certifying companies, they are aligned with the current market due to recent editions and require the support of Top Management for having a top-down approach. Regarding the differences, it was verified that ISO 31000 is direct and objective and COSO ERM has a long-winded character. On the other hand, ISO 31000 emphasizes theoretical aspects of risk management; COSO ERM emphasizes the practical aspects. COSO ERM's focus on risk factors and the ease of ISO 31000 integration with ERP systems are the last two differences identified in this study.

Based on the findings and conclusions, it can be argued that the field would benefit from further research on topics concerning COSO ERM and ISO 31000. In addition, students and researchers need to do more research and publications on the relationship between risk and quality management. Moreover, it would be interesting to analyze how managers are dealing with these two frameworks and how the integration with ISO 9001 can contribute to the achievement of their strategic objectives.

Despite of the findings uncovered, this article has some limitations regarding its method and nature. For instance, this is only a exploratory study, in which the descriptive analyzes of the documents are of subjectivity by nature. Given the limitation presented, further research is suggested to continue the conversation regard the topic. For instance, in addition to applying a quantitative methodology, we suggest to explore the shared role of COSO ERM and ISO 31000 from different perspectives.

REFERENCES

ABDUL RAHMAN, A. A.; AL-DHAIMESH, O. H. A. The effect of applying COSO-ERM model on reducing fraudulent financial reporting of commercial banks in Jordan. **Banks and Bank Systems**, v. 13, n. 2, p. 107–115, 2018.

ANDRADE ABREU, W. R.; ZOTES, L. P.; FERREIRA, K. M. Risk management in the evaluation of investment projects in startup. **SISTEMAS & GESTAO**, v. 13, n. 3, p. 267–282, 2018.

ANNAMALAH, S. et al. Implementation of Enterprise Risk Management (ERM) framework

in enhancing business performances in oil and gas sector. **Economies**, v. 6, n. 1, 2018.

AVEN, T.; YLONEN, M. The strong power of standards in the safety and risk fields: A threat to proper developments of these fields? **Reliability Engineering & System Safety**, v. 189, n. 1, p. 279–286, 2019.

AVEN, T.; ZIO, E. Foundational issues in risk assessment and risk management. **Risk Analysis**, v. 34, n. 7, p. 1164–1172, 2014.

BARAFORT, B.; MESQUIDA, A.-L.; MAS, A. Integrating risk management in IT settings from ISO standards and management systems perspectives. **Computer Standards and Interfaces**, v. 54, p. 176–185, 2017.

BJÖRNSDÓTTIR, S. H. et al. The Importance of Risk Management: What is Missing in ISO Standards? **Risk Analysis**, v. 0, n. 0, p. 1–33, 2021.

BOLANOS, E. et al. Risk Management and Anti-Bribery: an operational approach from the perspective of ISO 31000 and ISO 37001. **Revista Universidad Empresa**, v. 21, n. 36, p. 79–118, 2019.

CALLAHAN, C.; SOILEAU, J. Does Enterprise risk management enhance operating performance? **Advances in Accounting**, v. 37, n. 1, p. 122–139, 2017.

CHAKRABORTY, A.; GAO, L.; SHEIKH, S. Corporate governance and risk in cross-listed and Canadian only companies. **Management Decision**, v. 57, n. 10, p. 2740–2757, 2019.

COSO. **Enterprise Risk Management—Integrating with Strategy and Performance.**New YorkCommittee of Sponsoring Organizations of the Treadway Commission, , 2017.

CROVINI, C.; SANTORO, G.; OSSOLA, G. Rethinking risk management in entrepreneurial SMEs: towards the integration with the decision-making process. **Management Decision**, 2020.

DIAS, A. A. DE S. P. A more effective audit after COSO ERM 2017 or after ISO 31000:2009? **Revista Perspectiva Empresarial**, v. 4, n. 2, p. 73–82, 2017.

GOVENDER, D. The use of the risk management model ISO 31000 by private security companies in South Africa. **Security Journal**, v. 32, n. 3, p. 218–235, 2019.

ISO. **ISO 31000:2018 Risk Management - guidelines**. 2. ed. [s.l: s.n.].

KARANJA, E. Does the hiring of chief risk officers align with the COSO/ISO enterprise risk management frameworks? **International Journal of Accounting and Information Management**, v. 25, n. 3, p. 274–295, 2017.

MARTINS, M. A. F. et al. Risk management policy: Brazilian health regulatory agency's case. **Revista do Serviço Público**, v. 69, n. 1, p. 7–31, 2018.

MUZAIMI, H.; CHEW, B. C.; HAMID, S. R. **Integrated management system: The integration of ISO 9001, ISO 14001, OHSAS 18001 and ISO 31000**. AIP Conference Proceedings. **Anais**...2017

OLECHOWSKI, A. et al. The professionalization of risk management: What role can the ISO 31000 risk management principles play? **International Journal of Project Management**, v. 34, n. 8, p. 1568–1578, 2016.

OLIVA, F. L. A maturity model for enterprise risk management. **International Journal of Production Economics**, v. 173, p. 66–79, 2016.

PATÉ-CORNELL, E.; COX, L. A. Improving risk management: from lame excuses to principled practice. **Risk Analysis**, v. 34, n. 7, p. 1228–1239, 2014.

PREWETT, K.; TERRY, A. COSO's Updated Enterprise Risk Management Framework- A Quest For Depth And Clarity. **Journal of Corporate Accounting & Finance**, v. 29, n. 3, p. 16–23, 2018.

PURDY, G. ISO 31000:2009 - Setting a new standard for risk management. **Risk Analysis**, v. 30, n. 6, p. 881–886, 2010.

RAMPINI, G. H. S.; TAKYIA, H.; BERSSANETI, F. T. Critical Success Factors of Risk Management with the Advent of ISO 31000 2018 - Descriptive and Content Analyzes. **Procedia Manufacturing**, v. 39, p. 894–903, 2019.

ROD, B. et al. From Risk Management to Resilience Management in Critical Infrastructure. **Journal of Management in Engineering**, v. 36, n. 4, 2020.

SAEIDI, P. et al. The impact of enterprise risk management on competitive advantage by moderating role of information technology. **Computer Standards and Interfaces**, v. 63, n. 1, p. 67–82, 2019.

SAFA, N. S.; VON SOLMS, R.; FURNELL, S. Information security policy compliance model in organizations. **Computers and Security**, 2016.

SOUZA, F. S. R. N. DE et al. Incorporation of international risk management standards into federal regulations. **Revista de Administração Pública**, v. 4, n. 1, p. 59–78, 2020.

SUYASA, G. W. A.; LEGOWO, N. The implementation of system enterprise risk management using framework ISO 31000. **Journal of Theoretical and Applied Information Technology**, v. 97, n. 10, p. 2669–2683, 2019.

THOMYA, W.; SAENCHAIYATHON, K. The effects of organizational culture and enterprise risk management on organizational performance: a conceptual framework. **International Business Management**, v. 9, n. 12, p. 158–163, 2015.

TORREGROSA, M. B.; SOLER, V. G.; PEREZ-BERNABEU, E. Integration methodology: ISO 9001, ISO 31000 AND SIX SIGMA. **3C Empresa**, v. 8, n. 1, p. 77–91, 2019.

VANASCO, R. R. The Foreign Corrupt Practices Act: an international perspective. **Managerial Auditing Journal**, v. 14, n. 4 / 5, p. 161–261, 1999.

WILLIAMSON, D. The COSO ERM framework: A critique from systems theory of management control. **International Journal of Risk Assessment and Management**, v. 7, n. 8, 2007.