FGV EBAPE

RAP
BRAZILIAN JOURNAL OF PUBLIC ADMINISTRATION

Incorporation of international risk management standards into federal regulations

Flávio Sergio Rezende Nunes de Souza[1]
Marcus Vinícius de Azevedo Braga[2]
Armando Santos Moreira da Cunha[1]
Patrick Del Bosco de Sales[1]

[1]Fundação Getulio Vargas / Escola Brasileira de Administração Pública e de Empresas, Rio de Janeiro / RJ – Brazil
[2] Universidade Federal do Rio de Janeiro / Instituto de Economia Rio de Janeiro / RJ – Brazil

The issue of risk management has gained attention in the field of administration due to the dissemination of international frameworks. In Brazilian federal public administration, risk management is a recent and expanding practice. This research analyzes how international corporate risk management frameworks have been adopted by the federal government through regulations and guidelines. The study adopts the concepts of coercive, normative, and mimetic forces from the neo-institutional theory, and examines the presence of international norms in the Brazilian regulations. Through a qualitative approach, content analysis in documents, norms, interviews, and seminars was used to identify traits of the COSO ERM and ISO 31000/2009 frameworks, which were chosen based on relevance. Results identify important actors pushing for the use of international frameworks, such as international organizations, professional associations, and public agencies, especially those related to government audits. Despite the strong international influence, the Brazilian norms are adapted to the organizations' context and allowing the maintenance of national autonomy.
Keywords: enterprise risk management; public administration; COSO ERM; ISO 31000; Brazil.

Incorporação de modelos internacionais de gerenciamento de riscos na normativa federal

O interesse no gerenciamento de riscos tem crescido continuamente, fortalecido pela disseminação de modelos internacionais. Na administração pública federal brasileira, o uso da gestão de riscos é recente e encontra-se em expansão. Esta pesquisa analisou como modelos internacionais de gerenciamento de riscos corporativos são adotados pelas normas e orientações do Governo Federal. Aplicam-se os conceitos de forças coercitivas, normativas e miméticas da teoria neoinstitucional e observa-se a presença de conceitos das normas internacionais na normativa brasileira. Aplicou-se a análise de conteúdo em documentos, entrevistas, normas e palestras, a fim de identificar traços do modelo do Comitê das Organizações Patrocinadoras de Treadway (*Committee of Sponsoring Organizations of the Treadway Commission* [COSO]) para Gerenciamento de Riscos Corporativos (*Enterprise Risk Management* [ERM]), conhecido como modelo "COSO ERM", e do modelo da Organização Internacional de Normalização (*International Organization for Standardization* [ISO]), conhecido como Norma ISO 31000:2009, adotados por sua relevância. Os resultados identificam que importantes atores exercem pressões para adoção dos modelos internacionais, como os próprios organismos internacionais, associações profissionais e órgãos públicos, em especial aqueles ligados à auditoria governamental. Apesar da forte influência verificada, a estruturação das normas permite a manutenção da autonomia nacional e sua customização no contexto das organizações.
Palavras-chave: gerenciamento de riscos corporativos; administração pública; COSO ERM; ISO 31000:2009; Brasil.

Incorporación de modelos internacionales de gestión de riesgos en las reglamentaciones federales

El interés en la gestión de riesgos ha crecido de manera constante, fortalecido por la difusión de modelos internacionales. En la administración pública federal de Brasil, el uso de la gestión de riesgos es reciente y se está expandiendo. Esta investigación analiza cómo las normas y directrices del gobierno federal adoptan los modelos internacionales de gestión de riesgos corporativos. Siguiendo la teoría neoinstitucional, se investigó la exposición a fuerzas coercitivas, normativas y miméticas, y la presencia de conceptos de normas internacionales en la reglamentación brasileña. Se utilizó el análisis de contenido en documentos, normas, entrevistas y seminarios para identificar los rasgos de los modelos COSO ERM e ISO 31000/2009, adoptados por su relevancia. Los resultados identifican actores importantes que ejercen presión para la adopción de modelos internacionales, como organizaciones internacionales, asociaciones profesionales y agencias públicas, especialmente las vinculadas a la auditoría gubernamental. A pesar de la fuerte influencia, la estructuración de estándares permite el mantenimiento de la autonomía nacional y su personalización en el contexto de las organizaciones.
Palabras clave: gestión de riesgos corporativos; administración pública; COSO ERM; ISO 31000-2009; Brasil.

DOI: http://dx.doi.org/10.1590/0034-761220180117x
ISSN: 1982-3134
Article received on April 04, 2018 and accepted on November 09, 2019.
[Original version]

1. INTRODUCTION

Enterprise risk management is considered to be an important instrument within the framework of corporate governance. It is also known as "new risk management" (Palermo, 2014). Enterprise risk management is the integral, formal and systematic use of risk management and it has been adopted by various types of organizations, including the public sector (Oulasvirta & Anttiroiko, 2017).

The diffusion, adoption and use of enterprise risk management, like managerial innovation, has been the focus of research during recent decades. It has been increasingly diffused abroad, reaching a variety of organizations throughout the world. However, studies related to the diffusion of this instrument in the public sector are still restricted to countries which have adopted it in an anticipated manner, which in general are considered developed (Collier & Woods, 2011; Crawford & Stein, 2005; Oulasvirta & Anttiroiko, 2017; Palermo, 2014; Woods, 2009).

This influence spans countries and internationally the norms and practices developed in and for one context have been applied to countries with different contexts. This study analyzes the influence of international models of enterprise risk management of Anglo-Saxon origin on the norms and orientations of the Brazilian federal government on this issue. It focuses on the two international models which are considered the most relevant: a) the *Committee of Sponsoring Organizations of the Treadway Commission* [COSO] for *Enterprise Risk Management* [ERM] model, known as "COSO ERM"; and b) the *International Organization for Standardization* [ISO]) model, known as "ISO 31000:2009". To do this, we have evaluated norms, documents and accords, as well as interviews and talks, using a qualitative approach through content analysis (Bardin, 2011).

The COSO consists of the main financial and accounting professional associations in the United States of America. The COSO ERM was developed by the British company PricewaterhouseCoopers (PwC), with the collaboration of a consultative board of American professionals (Hayne & Free, 2014). ISO 31000:2009, on the other hand, is derived from a model created by the Australia/New Zealand Standards Committee [AS/NZS]), known as Norm AS/NZS 4360:2004 (Leitch, 2010). These models of Anglo-Saxon origin were born from searches for fraud in financial/accounting reports (Delmas, 2002; Delmas & Montes-Sancho, 2011; Delmas & Montiel, 2008; Guler, Guillén, & Macpherson, 2002; Hayne & Free, 2014).

The incorporation of the foreign models doesn't guarantee that the implementation of risk management will be successful. Various environments and cultures need to adapt the content of these models to adjust their object of focus, with the risk of straying from the end sought by the norm (Dobija, 2015; Oulasvirta & Anttiroiko, 2017).

In addition to contributing to the literature dealing with Latin America's late adoption of these standards, this article helps understand the process of normalizing enterprise risk management in the Brazilian federal government, highlighting the forces and actors involved in this process.

2. THE ADOPTION OF MANAGERIAL INNOVATIONS IN THE INTERNATIONAL CONTEXT

Recent studies deal with the dissemination of the voluntarily adopted models which define and regulate activities (Hayne & Free, 2014), for example, various ISO norms (Delmas, 2002; Delmas & Montes-Sancho, 2011; Delmas & Montiel, 2008; Guler et al., 2002) and the COSO ERM model (Hayne & Free, 2014), among others (Durand & McGuire, 2005; Perez-Aleman, 2010). According to Rogers (1995, p. 5), diffusion consists of a "process through which innovation is communicated by certain channels over time by members of a social system."

The neo-institutional approach predominates in the explanation of the diffusion of international models (Guler et al., 2002; Perez-Aleman, 2010). It emphasizes diffusion by way of isomorphism which is a product of coercive, imitative and normative forces, which conduct the adaptation of organizational characteristics with the environment (DiMaggio & Powell, 1983).

The coercive type is derived by exogenous pressures, exercised by other organizations and the cultural expectations of society. It may manifest itself through persuasion or an invitation to act jointly, in addition to technical and legal requirements. In this manner, various countries, as well as international organizations and development agencies, can impose their expectations on government, which often are pressured to meet standards which are considered legitimate (DiMaggio & Powell, 1983; Dobbin, Simmons, & Garrett, 2007; Weyland, 2005). Thus, imitative isomorphism occurs when an organization takes what other organizations are doing in terms of solutions for problems, such as the model. Normally this occurs when technologies are insufficiently understood or there is uncertainty in the environment. The reproduction of the characteristics of these organizations may be involuntary or explicit, and can be made viable by consulting firms or professional associations. Companies adopt the practices of these organizations to increase their legitimacy, to demonstrate that they are improving their processes. Finally, normative isomorphism is related to professionalization, given that members of certain professions tend to define work methods. It should be noted that these professional categories suffer imitative and coercive pressures. The sources of this isomorphism are related to education and a cognitive base. Thus, it is professional networks which diffuse organizational models seen as legitimate by their adopters, due to the approval of these networks.

Applying these concepts to the organizational field in the public sector, governments seek legitimacy through the adoption of characteristics of global solutions that are already accepted and legitimized (Meyer, Boli, Thomas, & Ramirez, 1997) or seek to imitate governments or institutions which have greater legitimacy (DiMaggio & Powell, 1983; Dobbin et al., 2007; Weyland, 2005). Thus, they emulate their peers or utilize models that are available, seeking those which are most notable and accessible (DiMaggio & Powell, 1983; Miller & Banaszak-Holl, 2005; Soule & Earl, 2001; Strang & Soule, 1998). Individuals in political positions end up depending on this legitimacy to defend the viability of their proposed solutions (Amenta & Ramsey, 2010). Finally, governments can adopt standardized procedures due to pressure from professional and academic associations, as well as private organizations which produce methodologies (DiMaggio & Powell, 1983; Hall, 1993; Strang & Soule, 1998).

Despite similar pressures, these answers may not appear at the same time. In developing economies, the adoption of international models tends to be delayed. This is explained in part due to innovation learning within other contexts, and the need to adapt innovation to the local context, which leads

to greater difficulties in its implementation, given the differences between material resources and knowledge or due to specific cultural differences (Perez-Aleman, 2010). These aspects apply to managerial innovations, such as risk management, whose adoption has intensified during the past 20 years, especially in relation to the COSO ERM and ISO 31000:2009 models (Huber & Scheytt, 2013; Scheytt, Soin, Sahlin-Andersson, & Power, 2006).

3. ENTERPRISE RISK MANAGEMENT MODELS

The model known as COSO II, "Enterprise Risk Management – Integrated Structure", was launched in 2004. The first model COSO[1], known as COSO I, arose in 1992 with the publication of the "Internal Control – Integrated Structure," but it is not considered enterprise risk management because its focus is internal control.

COSO II does not substitute the previous version, but rather incorporates issues of internal control and introduces risk management through new components and incorporated elements. In the conception phase, COSO II counted on the assistance of PwC and a consultative board, made up of consultants, academics and executives. At the time of its launch, COSO already had a good reputation due to its historical success in establishing guidelines and best practices (Hayne & Free, 2014). The updating of COSO II in 2017 preserved the main aspects of the previous version and made its text clearer and broader. In addition, this version includes aspects of managerial and strategic culture, such as a broader vision of objectives and organizational levels, in a way that enables organizations to get more out of enterprise risk management (*Committee of Sponsoring Organizations of the Treadway Commission* [COSO], 2017).

The ISO[2] 31000:2009 (*International Organization for Standardization* [ISO], 2009) on the other hand, was developed by a special committee, made up of delegations from 28 countries. They improved the concepts, guidelines and practices of technical norms which preceded them such as AS/NZS 4360:2004, established by the joint committees of Australia and New Zealand which led to the original international norm (Leitch, 2010). Unlike COSO II, this norm does not take a prescriptive approach, instead offering general principles and guidelines in terms of enterprise risk management.

These models are quite similar and do not present conflicts between each other, and should become further aligned in the next few years (Moeller, 2011). There are more similarities than differences between the two models. However, ISO 31000:2009 offers a more simplified approach (Gjerdrum & Peter, 2011). Box 1 presents the similarities identified between the models and Box 2 presents a few differences.

[1] COSO is a non-profit committee dedicated to the improvement of financial reports through ethics, the effectiveness of internal controls and corporate governance, and it arose with the mission to create systematic structures which address the new scenario presented by corporations. It is formed by some of the main financial and accounting professional associations of the United States.

[2] ISO is a world forum which seeks consensus in the elaboration of international norms through the conciliation of interests of a variety of segments within society. Its norms are developed through various national organizations of normalization, currently present in more than 150 countries.

BOX 1 SIMILARITIES BETWEEN COSO ERM AND ISO 31000:2009 FRAMEWORKS

Aspect	Description
Scope	Applicable to the entire organization and at lower organizational levels. Can be used in any type of organization.
Risk concept	Risk is positive and negative (opportunities and threats).
Documentation	Requires the establishment of a risk management policy. Requires the establishment of risk assessment criteria. States that all risk management activities should be documented.
Characteristics	The implementation of risk management takes into account the specific needs of the organization. Dynamic, iterative process that contributes to continuous improvement. Integration of risks with objectives. Risk management is incorporated into organizational processes. Need to consider cost-benefit in the treatment of risks. The risk management process does not guarantee the achievement of objectives.
Process	Establishment of context / objectives, identification, analysis and evaluation, treatment, communication and monitoring.

Source: Elaborated by the authors.

In terms of the differences, it should be emphasized that in terms of responsibility, while COSO defines specifically who is involved, ISO lets the organization define the central roles. Still, in relation to the roles, it appears that the elevated involvement of auditing professionals in the use of the models makes them transcend this functions, and enables them to perform consulting activities for organizations (Zwaan, Stewart, & Subramaniam, 2011).

BOX 2 DIFFERENCES BETWEEN THE COSO ERM AND ISO 31000:2009 FRAMEWORKS

Aspect	COSO ERM	ISO 31000:2009
Guidance	Detailed and prescriptive.	Generic principles and guidelines.
Publication	By entities of accounting and auditing professionals.	Procedure for creating ISO standards (consensus).
Responsabilities	Establishes specific responsibilities. Defines roles of CEO, Board of Directors, internal auditors, senior and other managers. States that the managers closest to the potential issues should be the risk owners.	At the discretion of the organization. Definition through establishment of policy, context and risk owners.

Source: Elaborated by the authors.

4. THE ADOPTION OF ENTERPRISE RISK MANAGEMENT BY THE PUBLIC SECTOR

Various studies address the diffusion and adoption of tools and systems, which initially were designed for private companies, but later were adopted by the public sector (Jackson & Lapsley, 2003; Oulasvirta & Anttiroiko, 2017; Spano, Carta, & Mascia, 2009; Troshani, Jerram, & Hill, 2011).

In particular, the adoption of enterprise risk management by the public sector has been discussed by some authors, for example public organizations in the United Kingdom, and local governments in Finland (Oulasvirta & Anttiroiko, 2017), the United Kingdom and Australia (Collier & Woods, 2011; Crawford & Stein, 2005; Woods, 2009).

In the case of local governments in Finland, risk management was applied mostly in specific areas such as health, security and finance, rather than the integral use of enterprise risk management, demonstrating the existence of "silos". In addition, Oulasvirta and Anttiroiko (2017) relate the lack of a perceived benefit on the part of managers when comparing the implementation costs of enterprise risk management. It has been verified that the pressures of voluntary adoption of the enterprise corporate risk management have not had the desired effect when senior managers do not adhere to the project. Thus, according to the authors, public sector organizations should be more selective about adopting management tools than they usually are (Oulasvirta & Anttiroiko, 2017).

Meanwhile in the United Kingdom, the introduction of enterprise risk management by local governments has been influenced by performance audits realized by the central government, which present expectations that enterprise risk management systems are based on already available professional model practices (Palermo, 2014; Woods, 2009).

5. METHODOLOGY

The data was collected by the examination of norms and documents, semi-structured interviews and seminars given by the National School of Public Administration (ENAP) about the challenges of implementing the Joint Normative Instructions of the Ministry of Planning, Development and Management (MPDG) and the Ministry of Transparency and the Federal Comptroller General's Office (CGU) No. 01/2016 (National School of Public Administration [ENAP], 2017). The data was then submitted to content analysis (Bardin, 2011).

First, we selected the norms which structure this subject in this country, including: a) the basic reference on governance (Federal Accounting Court [TCU], 2014); b) Law No. 13,303 (2016); c) the Joint Normative Instruction MP/CGU No. 1 (2016); d) the Federal Accounting Court's reference on the combat of fraud and corruption (TCU, 2017a); and e) the Federal Comptroller General's Normative Instruction No. 3 ([CGU], 2017). In the codification of the comparative analysis (Gibbs, 2008), the characteristics presented in Boxes 1 and 2 were utilized.

Then, we observed the concepts and recommendations of the international models reflected in the norms and the decisions of the Federal Accounting Court (TCU). We then used the TCU's database (TCU, 2017b), which identified the number of citations and conditions under which the international models are cited or referenced in the documents or accords of this government body. The search was conducted in September 2017 and used the keywords "COSO" and "risks" in combination, and the term "31000" in isolation. The collection resulted in 185 accords and 4 normative acts, with the first occurrences appearing in 2006, and most of the references related to COSO I. The COSO II and ISO models appeared beginning in 2010. In relation to the normative acts, two dealt with both models

and two referred exclusively to COSO ERM. In terms of the accords, 43 did not mention these models and most of these were related to COSO I. Of the other accords, 25 treated both models, 99 treated just COSO II and 18 dealt exclusively with ISO 31000:2009.

Finally, we conducted interviews to complement the documentary analysis with six specialists in risk management as illustrated in Box 3. It should be noted that the first two interviewees participated directly in the elaboration of the Joint Normative Instruction MP/CGU No. 1 (2016).

BOX 3 INTERVIEWS CONDUCTED

Interviewee	Interviewee Description	Public/private service experience (years)
I1	Federal public servant	31
I2	Federal public servant	10
I3	Private consultant	38
I4	Federal public servant	20
I5	Federal public servant	31
I6	Federal public servant	20

Source: Elaborated by the authors.

A variety of data sources and treatment methods were employed to obtain the triangulation methodology (Flick, 2007).

6. ENTERPRISE RISK MANAGEMENT ADOPTION INITIATIVES BY THE FEDERAL GOVERNMENT

The process of adopting enterprise risk management by the federal government was largely addressed in 2016, even though it was initiated in the 1990s. In the initial phase, few government bodies were involved with the model. After the issue was normalized by Joint Normative Instruction MP/CGU No. 1 (2016), the implementation of this tool became prevalent in the federal Executive Branch.

The first initiatives took place in a fragment fashion in several organizations of the federal government. The Central Bank in the 1990s, after the advent of the Real Plan, initiated financial risk management. In 2011, according to several of the interviewees (I1 and I2) and a talk (ENAP, 2017), the Central Bank began to use enterprise risk management in a broader fashion.

According to one of the interviewees (I2), during the beginning of the first decade of the 21st century, initiatives by the Ministry of Social Security and the Secretariats of the National Treasury and Internal Revenue were presented in the federal sphere, and in 2013 enterprise risk management was presented by the National Program of Public Management and Debureaucratization (Decree No. 5,378, 2005), which was discontinued in 2017. This program published a manual (Ministry of Planning, Development and Management [MPDG], 2013), based on the British Treasury's *Orange Book* (*Her Majesty's Treasury [HM Treasury*], 2004). However, according to some of the interviewees (I1, I2), the use of this methodology was voluntary and did not achieve relevant dissemination on this occasion.

More structured initiatives have permitted an expansion of enterprise risk management in public management, as has occurred in the Federal Accounting Court, the Federal Comptroller General's Office and then the Ministry of Planning, Development and Management. For example, in 2009, seeking to support a bill, the Federal Accounting Court conducted a study of internal controls, exploring models and verifying whether other countries have amplified their role, coming to treat them as risk management instruments. In 2011, the Federal Accounting Court established the improving of enterprise risk management as a strategic objective. According to the interviewees (I3), the subject continued to be a subject of interest in strategic planning in 2015.

An important mark in the history of the Federal Accounting Court was the application of a questionnaire in 2013 to evaluate the maturity of risk management in 65 organizations of indirect administration. The response of these bodies favored reflection about this subject. At the same time, according to one of the interviewees (I1), the fact that the Federal Accounting Court realized this study at the time, demonstrated that the court supported this approach. Thus, the establishment of technical requisites and the expectations of this body in regard to this subject placed a coercive and at the same time normative pressure on professionals within the governmental auditing area.

For the Federal Comptroller General's Office, an important mark in its history was an invitation made to the Organization of Economic Cooperation and Development (OECD) in 2009. It paid a visit and produced a report on the Brazilian federal public administration's system of integrity (ENAP, 2017; *Organisation for Economic Cooperation and Development* [OECD], 2012). One of the recommendations of the report was to "integrate risk management as a key element of responsible management, and as a way to promote integrity and prevent improbity, embezzlement and corruption" (OECD, 2012, p. 19). The report pointed out gaps in risk management and highlighted the guiding role of the Federal Comptroller General's Office (CGU). With this, the subject was studied in a more intense manner by the CGU. These efforts were contemplated with financing from the Interamerican Development Bank (IDB) in its program to Strengthen Prevention and Combat Corruption in Brazilian Public Management, which, among other subjects, includes risk management. In 2012 it formed a working group which sought to establish a methodological reference for risk management in public administration (I1).

In 2016, Minister Valdir Simão, ex-minister of the CGU and then Minister of Planning, who accompanied the work of the OECD, proposed the implementation of risk management for the instrumentalization of public managers (I1). In this manner, together with the CGU, led at the time by Minister Luiz Navarro, who also accompanied the work of the OECD, he decided to elaborate the publication of the Joint Normative Instruction MP/CGU No. 1 (2016), normalizing the application of this methodology in the federal Executive Branch (I1, I2). This agenda led to other important events related to this subject as reflections of federal public administration, culminating in the publication of Decree No. 9,203 (2017), and the preparation of a bill in which management risk is explicitly addressed (I1).

7. ANALYSIS OF NORMS, GUIDELINES AND ACCORDS

This study has revealed a greater presence of the COSO model in the analyzed documents. The COSO model appeared before the ISO model and soon won recognition, initially as a discussion of internal controls. This model is sponsored by five important American organizations, including the Institute

of Internal Auditors (IIA) which demonstrates its popularity among professional auditors. It is also supported by the International Organization of Supreme Audit Institutions (INTOSAI), by the IDB, by the Work Bank and the Government Accountability Office (GAO) of the United States (TCU, 2009).

Meanwhile, ISO 31000:2009 appeared only in 2009. According to one of the interviewees (I1), ISO offers a more practical approach, while COSO is more doctrinaire. Another point in favor of this model is that the ISO, as an international normalization organization, was better known than COSO, given that it is present in various countries and contains a definition of norms of the most varied natures, such as metrology, food safety, quality systems and environmental protection, among others.

The acceptance of these models, according to some of the interviewees (I1, I4), was facilitated by organizations of elevated prestige conceiving and supporting these models which confers legitimacy on them, providing security for anchoring enterprise risk management in the public sector. Another interviewee (I4) points out the use of these models facilitates the standardization of concepts and language.

The mention of these models in these norms and accords demonstrates the influence that they possess. In evaluating the significance of the excerpts present in these documents, we verified mainly the recommendations of how to apply these models and the recognition that they are important references for enterprise risk management due to their legitimacy, credibility and acceptance. Box 4 shows examples of these excerpts.

BOX 4 INFLUENCES OF FRAMEWORKS ON RISK MANAGEMENT PRACTICES IN THE BRAZILIAN ADMINISTRATION

Document	Quote within document
Port. 189/2009 of TCU (TCU, 2009a)	*'[...] the **use of the COSO framework as a reference** for analysis, emphasizing **enterprise risk management**, based on principles of good governance [...]' (p. 2).*
Court ruling 1233/2012 record 19/2012 - plenary (TCU, 2012)	'[...] these countries adopt convergent internal control frameworks, based on risk management and governance structures [… The] frameworks are based on the main documents ***related to internationally recognized risk management and internal controls, such as the COSO I / II***, the AS / NZS 4360 standard, and Intosai's Guidelines for the Internal Control of the Public Sector. [...] was concluded with a suggestion of a draft legislative proposal for the amendment of the Fiscal Responsibility Law, including a section dealing with "Risk Management, Internal Control and Corporate Governance", which contributes for inclusion within the Brazilian legal system of good practices for proper corporate governance contained in ***benchmarks such as Coso I and II, recognized worldwide***.'
Court ruling 7128/2013 record 43 - second chamber (TCU, 2013)	*'[...] the promotion of risk assessment work, **using as a reference consecrated frameworks such as Coso II** [...]'*

Continue

Document	Quote within document
Court ruling 242/2015 record 5/2015 - plenary (TCU, 2015a)	*'As an audit criteria, and in order to enable for a comprehensive analysis of the theme,* ***well-established risk assessment and controls frameworks****, in particular the* ***Coso ERM framework and the ABNT NBR-ISO 31000: 2009*** *standard, were used as reference. […] The Coso ERM […] was designed to disseminate risk and control awareness across the entity and become a common framework for discussion and assessment of organizational risks. […] compliance and implementation of its recommendations on internal control are widely used and remain as a* ***model in Brazil and in most countries of the world****.* *[...] ABNT NBR-ISO 31000:2009 [...] is* ***usually adopted as a reference for benchmarking*** *processes associated with risk management.'*
Court ruling 1294/2015 record 19/2015 - plenary (TCU, 2015b)	*'[...] developed based on international models (****in particular the Coso ERM and ISO 31000/2009****) […]'*
Court ruling 729/2017 record 12/2017 - plenary (TCU, 2017c)	*'[...] considering the recommendations of* ***international best practices for enterprise risk management****, such as* ***COSO / ERM****, INTOSAI GOV 9130/2007 and ABNT NBR I****SO 31000: 2009*** *standards; [...] incorporating into its text* ***the best international practices established in this area*** *[…] the main risk management frameworks such* ***as ISO 31000/2009*** *and frameworks of the Committee of Sponsoring Organizations of the Treadway Commission -* ***COSO I and II*** *[...]'*

Source: Elaborated by the authors.

In the mentioned excerpts, the model is associated with: a) "best international practices"; b) "a reference for the realization of a benchmark"; c) "established models"; d) "internationally recognized [models]"; and e) "milestones", which at the same time confer legitimacy on the models, norms and constructed understandings, because they are based on something legitimate which is accepted internationally.

In our research, other models were also mentioned, but with less frequency than the studied models, as can be seen in Box 5. These models have a strong relationship with the two models studied here, with the exception of the United Kingdom model, which recognizes other models, but doesn't affirm that it is based on them.

BOX 5 OTHER FRAMEWORKS IDENTIFIED IN COURT RULINGS

Framework	Reference to the COSO and ISO 31000:2009 frameworks
INTOSAI GOV 9130	Focused in public sector activities and said to be based on COSO II (International Organization of Supreme Audit Institutions [INTOSAI], 2007, p. 5). Some court rulings refer to COSO INTOSAI.
AS/NZS 4360/2004	A precursor to ISO 31000/2009 developed by the standards bodies of Australia and New Zealand (Leitch, 2010).

Continue

Framework	Reference to the COSO and ISO 31000:2009 frameworks
Canadian	A guide to the implementation and operation of enterprise risk management within the Canadian government. Alignment with ISO 31000 demonstrated in item 2.2, quoted: *"the framework […] reflects, where appropriate, international and national standards related to risk management including the ISO 31000 Risk Management Standard"* (Government of Canada, 2012).
GAO	Specifically applicable to public sector activities, with a focus on internal controls and a strong influence from COSO I. Principles of COSO were adapted to suit a governmental environment (Government Accountability Office [GAO], 2014).
UK Treasury	Specifically applicable to the public sector, it provides general guidelines on enterprise risk management. Acknowledges the lack of enterprise risk management standard in government organizations and suggests organizations may opt to adopt frameworks such as AS/NZS 4360/2004, COSO ERM and the Canadian framework (HM Treasury, 2004).

Source: Elaborated by the authors.

Using the factors presented in Boxes 1 and 2, we found various aspects of the studied models in the principal norms selected, which guide enterprise risk management in the Brazilian federal administration. Box 6 describes the analysis realized with publications that address enterprise risk management as one of their subjects, which is to say, they are not specific.

BOX 6 FEDERAL GOVERNMENT NORMS ADDRESSING RISK MANAGEMENT

Norms	Description
Basic Governance Reference Applicable to Public Administration Bodies and Entities	Brings several aspects of risk management as a matter related to governance. Quote both frameworks in its text, and states that COSO II "is still *used as a reference in the topic of risk management"* (TCU, 2014, p. 4). Includes a *"risk management and internal control"* section. Conceptualizes risk by referring to ISO 31000. Cites COSO II and INTOSAI GOV 9130 (TCU, 2014, p. 26). Practices akin to those of the COSO and ISO 90001:2009 frameworks, e.g., a requirement to establish policy and ensure that risk management is part of the organizational processes.
Law 13.303/2016	Establishes governance practices for government and mixed-capital companies, as well as their subsidiaries. Includes ERM responsibilities.
IN 03/2017 - CGU	Establishes principles and guidelines for internal auditing, including ERM assessment. Risk management addressed within the management process (CGU, 2017).

Source: Elaborated by the authors.

Two of the norms analyzed have risk management as their main subject: a) the reference to combat fraud and corruption (TCU, 2017a), which is specific to risks related to this subject; and b) Joint Normative Instruction MP/CGU/PR No. 1 (2016), which offers general guidelines which determine the implementation of risk management in the context of all the bodies and entities of the federal Executive Branch.

The reference to combatting fraud and corruption directly cites the studied models, recommending their use. In addition, it points out that COSO is the dominant risk management model in the international corporate scenario, especially in the United States, and dedicates a specific topic to the Brazilian technical norm (NBR) ISO 31000:2009. In addition, it states that adaptations of these models have given origin to models applied to the public sector, including, for example, the GAO model (TCU, 2017a).

Some excerpts of Joint Normative Instruction MP/CGU/PR No.1 (2016) are practically identical to the models analyzed here, including, for example, the principle that deals with "systematic, structured and opportune" risk management (ISO, 2009, p. 7). Moreover, it adopts a model structure made up of components, which are identical to the components of COSO ERM (*Committee of Sponsoring Organizations of the Treadway Commission* [COSO], 2004, p. 7). This perception is confirmed by the Federal Accounting Court (2017a, p. 25): "that the risk management part of this [Normative Instruction] is based on Coso II".

The perception of the interviewees (I1, I2, I3), especially those who participated in the elaboration of Joint Normative Instruction MP/CGU/PR No. 1 (2016), is that the main references used in the elaboration of the instruction are COSO and ISO 31000:2009. One of the interviewees (I2) added that the *Orange Book* (HM Treasury, 2004) was used as one of the main references.

Box 7 illustrates the characteristics of these norms related to the studied models.

BOX 7 CHARACTERISTICS OF ENTERPRISE RISK MANAGEMENT GUIDANCE NORMS IN THE FEDERAL GOVERNMENT

Normative guideline	IN 01/2016 – MP/CGU - Covers internal controls, risk management and governance within the Federal Executive Branch.	Reference for combating fraud and corruption: applicable to public administration bodies and entities
Scope	All bodies and entities: *"Art. 1 The bodies and entities of the Federal Executive Branch shall adopt measures for the systematization of practices related to risk management, internal controls, and governance".* Art. 3 § 3 *"Components for the internal management control and risk management shall apply to all levels, units and dependencies of the body or public entity".*	An organization's risk management system shall cover all organizational levels in an integrated manner. *"Must be integrated with the organization's risk management activity, which is a broader activity because that includes a systemic view of most relevant risks the organization is exposed to".* (TCU, 2017a, p. 23).; *"[…] the reference was designed to assist any public organization"* (TCU, 2017a, p. 12).

Continue

Normative guideline	IN 01/2016 – MP/CGU - Covers internal controls, risk management and governance within the Federal Executive Branch.	Reference for combating fraud and corruption: applicable to public administration bodies and entities
Risk concept	Art. 2, XIII – *"risk: possibility of occurrence of an event that will have an impact on the fulfillment of the objectives"*.	Risk management accepts positive and negative outcomes, as described in the COSO and ISO 31000:2009 frameworks. *"To minimize, monitor and control the likelihood and impact of negative events or maximize the use of opportunities"* (TCU, 2017a, p. 24).
Documentation	Risk management policy covered in section IV, for the implementation by Federal Executive Branch organizations.	The risk management policy applies because it states that it must be integrated with the organization's risk management, and mentions IN 01/2016.
	The policy should establish risk management criteria specified in Art. 17, II, b) *"how and with what frequency the risks will be identified, evaluated, treated and monitored"*.	*"This stage also defines the scope and risk criteria for the rest of the process"* (TCU, 2017a, p. 27).
	Implementation of policy and guidelines subject to CGU auditing requires appropriate documentation to be produced.	*"Documenting and assigning responsibility for risks and controls is important"* (TCU, 2017a, p. 28).
Characteristics	Art. 3º § 5º *"Appropriate internal management controls [...] shall be integrated into the management process, commensurate to the extent of the risks, taking into account the nature, complexity, structure and mission of the body or public entity"*.	*"Anti-fraud and anti-corruption measures should not be applied uniformly and indistinctly in all organizations. Each organization should assess appropriate measures against expected risks and benefits, taking into account an organization's size, nature and complexity"* (TCU, 2017a, p. 32).
	Art. 14, I *"Risk management in a systematic, structured and timely manner [...]". Art. 14, V "[...] support for continuous improvement of organizational processes"*.	*"Implemented and applied in a systematic, structured and timely manner"* (TCU, 2017a, p. 24).
	Art. 15, II *"increase the likelihood of achieving an organization's objectives by reducing risks to an acceptable level"*.	*"[…] manage risks [...] in order to create the conditions to achieve objectives and fulfil purposes"* (TCU, 2017a, p. 24).
	Art. 14, V *"Use of risk management to support the continuous improvement of organizational processes"*.	*"Should be considered by the organization during its activities"* (TCU, 2017a, p. 22).
	Art. 14, III *"Establishment of internal control procedures proportionate to risk, observing cost-benefit ratios, and intending to add value to the organization"*.	*"The benefit from the implementation of anti-fraud and anti-corruption controls should be greater than its cost"* (TCU, 2017a, p. 33).
	It does not guarantee the achievement of objectives. Art 2º, VII *"[...] provide reasonable certainty as to the achievement of an organization's objectives"*.	*"[...] increase effectiveness in achieving objectives"* (TCU, 2017a, pp. 25-26).
Process	Section III follows the components of COSO ERM accurately, i.e., internal environment; goal setting; identification of events; risk assessment; response to risks; activities of internal controls; information and communication; monitoring.	*"[…] identifying [risks], analyzing them, and then evaluating whether they should be modified by any criterion"* (TCU, 2017a, p. 24).

Continue

Normative guideline	IN 01/2016 – MP/CGU - Covers internal controls, risk management and governance within the Federal Executive Branch.	Reference for combating fraud and corruption: applicable to public administration bodies and entities
Guidance	General guidelines	Describes mechanisms and components specifically designed to combat fraud and corruption.
Publication	MP e CGU (Administration and Internal Audit).	TCU (External Audit).
Responsabilities	Responsibilities covered throughout the text and specifically in section V.	Assignment of responsibilities to be coordinated.

Source: Elaborated by the authors.

Joint Normative Instruction MP/CGU No. 1 (2016) offers general guidelines so that the government bodies can have a certain amount of autonomy in customizing their risk management models. According to the understanding of the interviewees (I1), the norm is doctrinaire; it does not establish a specific rite, and maintains flexibility for use in various types of organizations. On the other hand, more specificity is observed in the studied models, with their having determinations in terms of responsibilities, the institution of committees and steps to follow. An example of this is the determination of the risk management policy that the entities should institute. They point out various aspects that should be present in the policy, and also determine a timeframe for them to be put into practice.

8. DIFFUSION ANALYSIS

The analysis of documents and norms related to the risk management of federal public administration indicates the prominence of control bodies in the incentives for managers to use this instrument. The Joint Normative Instruction MP/CGU No. 1 (2016) itself corroborates the role of internal auditing in spreading the application of risk management in Art. 2, III: "[...] it assists the organization in realizing its objectives, based on the application of a systematic and disciplined approach to evaluate and improve the efficiency of risk management processes [...]". This result is in line with the trends observed by Maijoor (2000), namely the growth of internal control systems, which are intimately related with risk management, and are part of the reforms undertaken by corporate governance in various nations, which also increases the relevance of internal auditors. The role of auditing can also be observed in other countries (Zwaan et al., 2011).

It has been verified that, in federal public administration, the oldest normalization that addresses enterprise risk management dates from 2014, and that the first accord to mention a specific model of enterprise risk management was released in 2010. This fact not only demonstrates how current this subject is in the country, but also as noted in one of the interviews (I1), the existence of a certain interval of time needed for the repercussion of international models in the Brazilian context, given that COSO ERM was launched in 2004. Another motive for this delay may be associated with rationality and selectivity in the adoption of managerial innovations in the public sector, as observed by Oulasvirta and Anttiroiko (2017). Using this same line of analysis, it was not possible to observe influences of the latest update to COSO ERM, which occurred in 2017, due to the short timeframe between its release and the development of the current study.

This chronology enables us to conclude that before managers paid attention to enterprise risk management, it was already a concern of the external control body. According to some of the interviewees (I1, I4), the auditors initiated their recommended practices basing their arguments on international models up until the moment of the effective institutionalization of enterprise risk management. In addition, the first normative instruction about this subject was published by the external control body (TCU, 2014). The Executive Branch regulated risk management only in 2016 in conjunction with the internal control body through Joint Normative Instruction MP/CGU No. 1 (2016).

In line with this, one of the interviewees (I4) reinforced the importance of the Federal Accounting Court in the introduction of enterprise risk management in federal public administration. In part, this pioneering role may be attributed to the international influence of INTOSAI: "the Federal Accounting Court, as a member of INTOSAI, also recognizes and uses the model [COSO I] as a base for its evaluations [...]" (TCU, 2009b, p. 10)[3]. Some of the interviewees (I1, I4, I5, I6) point out, in the same line, the role of professional associations as important diffusors of these models.

Thus, normative isomorphism is very much present, in view of the strong structure of the professional categories dealing with enterprise risk management. In the Brazilian public sector, enterprise risk management appeared mainly in audit related bodies, even though risk constitutes a concern for managers. In this area, the COSO is very well known, and has been for a long time, due to the use of COSO I. It is present in universities and is part of the repertoire of professionals in the accounting and auditing area.

Enterprise risk management is a very recent instrument, especially in the public sector. Thus, an insufficient knowledge of this instrument also favors imitative isomorphism, through the adoption of available models of easy use, such as those studied here.

The interviewees mentioned their own personal experiences with studies of these models in academia. Some of them (I2, I5) took courses on these specific models, such as AS/NZS 4360:2004. Another studied them on his own (I1). The interviewees were teachers of specialized courses in the Federal Comptroller General's Office in 2008 and 2009 (p. ex., I1), and in private courses, which have been sought after by civil servants (for ex., I5). It may also be observed in the dissemination of knowledge through personnel hiring processes. Some of the interviewees obtained knowledge about enterprise risk management when they were in one governmental body and again when they used them in another (I2, I4).

Thus, in accordance with imitative isomorphism, we have verified that the use of these models occurs in an involuntary manner through civil servants who have had access to these models through classes, talks and training. It also occurs in a voluntary manner, given that large consulting firms promote these models, such as, for example, PwC, which participated in the elaboration of COSO ERM. In addition, international organizations and agencies, such as the OECD, have recommended the use of these enterprise risk management instruments in Brazil. Thus, there is evidence of influence related to coercive isomorphism. In the same way, coercive pressures are observed in the expectations of the control bodies themselves.

[3] In 2007, INTOSAI updated its guidelines for public sector control standards incorporating COSO II (INTOSAI, 2007).

It should be emphasized that the efforts made to implement a broad model in terms of the norms and guidelines of the federal government, contemplating risks in an integral fashion in its diverse units, avoids a fragmented approach to risk management by sectors as observed in the Finnish case (Oulasvirta & Anttiroiko, 2017).

9. CONCLUSIONS

We have observed the strong influence of international models, as expected. Models such as the COSO ERM and ISO 31000:2009 have been used as a base for efforts to implement enterprise risk management in the federal public administration, in search of an internationally accepted legacy. However, the presence of models considered to be international references in the normative instructions of the Federal Accounting Court and other federal bodies, does not guarantee their application. Their effective adoption depends on various factors, such as leadership and instrument promotion (Oulasvirta & Anttiroiko, 2017). Since risk management uses a different logic of action in the public sector, it may be difficult to institutionalize. One example of this is offered by Azevedo, Aquino, Lino and Cavelmoretti (2019): risk management and mandatory measures according to Complementary Law No. 101 (Law of Fiscal Responsibility, 2000) are realized in a ceremonial manner by the analyzed governments. In other words, its adoption is not effective.

Despite the coercive and normative forces which have led risk management to be included in the normative instructions of the federal government and external control bodies, the real adoption of risk management in a general manner by executive bodies under public management still seems to be a distant step.

The influence of the Anglo-Saxon risk management models analyzed is not necessarily that of a specific country, but of international organizations which promote and disseminate these practices. The COSO model is sponsored by American associations and elaborated by one of the Big 4 auditing firms, PwC, which is based in London, while the ISO model has roots in the model previously elaborated by Australia and New Zealand.

The organizations which legitimize the adoption of these norms are international and of a professional nature. Among them we find: a) non-governmental organizations (NGOs) who act internationally, for example the OECD and the IDB; b) consultants and consulting firms; c) academia; d) professional associations, mainly those related to the accounting profession and the auditing area, such as INTOSAI and the IIA; and e) the government's own bodies and specialists, considered references due to their technical capacity.

It should be noted that despite the fact that the Brazilian norms studied present strong links with international models, the way in which they are structured, as general guidelines, makes it possible to maintain national autonomy and customize them within organizational contexts. Future research can examine the institutionalization (successful or not) of enterprise risk management in public sector organizations and how it has changed the behavior of managers and the conduct of public policies, services, and the type of control exercised by the internal bodies of these organizations.

REFERENCES

Amenta, E., & Ramsey, K. M. (2010). Institutional theory. In K. T. Leicht, & J. C. Jenkins (Eds.), *Handbook of politics: State and society in global perspective* (pp. 15-39). New York, NY: Springer.

Azevedo, R. R., Aquino, A. C. B., Lino, A. F., & Cavelmoretti, G. (2019). A precariedade do conteúdo informacional dos anexos de riscos fiscais de municípios brasileiros. *Advances in Scientific and Applied Accounting*, *12*(2), 4-22.

Bardin, L. (2011). *Análise de conteúdo*. Lisboa, Portugal: Ed. 70.

Collier, P. M., & Woods, M. (2011). A comparison of the local authority: adoption of risk management in England and Australia. *Australian Accounting Review*, *21*(2), 111-123.

Committee of Sponsoring Organizations of the Treadway Commission. (2004). *Enterprise risk* management: integrated framework. Jersey City, NJ: Author.

Committee of Sponsoring Organizations of the Treadway Commission. (2017). *Enterprise risk management: integrating risk with strategy and performance*. Jersey City, NJ: Author.

Crawford, M., & Stein, W. (2005). "Second order" change in UK local government: the case of risk management. *International Journal of Public Sector Management*, *18*(5), 414-423.

Decreto n. 5.378, de 23 de fevereiro de 2005. (2005). Institui o Programa Nacional de Gestão Pública e Desburocratização – GESPÚBLICA e o Comitê Gestor do Programa Nacional de Gestão Pública e Desburocratização, e dá outras providências. Brasília, DF.

Decreto n. 9.203, de 22 de novembro de 2017. (2017). Dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional. Brasília, DF.

Delmas, M. (2002). The diffusion of environmental management standards in Europe and in the United States: an institutional perspective. *Policy Sciences*, *35*, 91-119.

Delmas, M., & Montes-Sancho, M. J. (2011). An institutional perspective on the diffusion of international management system standards: the case of the environmental management standard ISO 14001. *Business Ethics Quarterly*, *21*(1), 103-132.

Delmas, M., & Montiel, I. (2008). The diffusion of voluntary international management standards: responsible care, ISO 9000, and ISO 14001 in the chemical industry. *Policy Studies Journal*, *36*(1), 65-93.

DiMaggio, P., & Powell, W. (1983). The iron cage revisited: institutional isomorphism and collective rationality in organizational fields. *American Sociological Review*, *48*, 147-160.

Dobbin, F., Simmons, B., & Garrett, G. (2007). The global diffusion of public policies: social construction, coercion, competition, or learning? *Annual Review of Sociology*, *33*(1), 449-472.

Dobija, D. (2015). Exploring audit committee practices: oversight of financial reporting and external auditors in Poland. *Journal of Management & Governance*, *19*(1), 113-143.

Durand, R., & McGuire, J. (2005). Legitimating agencies in the face of selection: the case of AACSB. *Organization Studies*, *26*(2), 165-196.

Escola Nacional de Administração Pública. (2017). *Seminário Gestão de Riscos: desafios para implementação da Instrução Normativa Conjunta MP/CGU* (video). Retrieved from: https://www.youtube.com/watch?v=Qvc-PoPxNyQ&t=3740s

Flick, U. (2007). *Managing quality in qualitative research*. London, England: SAGE.

Gibbs, G. (2008). *Analyzing qualitative data*. London, England: SAGE.

Gjerdrum, D., & Peter, M. (2011). The new international standard on the practice of risk management: a comparison of ISO 31000:2009 and the COSO ERM framework. *Risk Management*, *31*(2), 8-13.

Government Accountability Office. (2014). *Standards for Internal Control in the Federal Government* (GAO-14-704G). Washington, DC: Author.

Government of Canada. (2012). *Guide to integrated risk management: a recommended approach for developing a corporate risk profile*. Retrieved from: https://www.canada.ca/en/treasury-board-secretariat/corporate/risk-management/guide-integrated-risk-management.html#toc1_1

Guler, I., Guillén, M., & Macpherson, J. M. (2002). Global competition, institutions, and the diffusion of organizational practices: the international spread of ISO 9000 quality certificates. *Administrative Science Quarterly*, *47*(2), 207-232.

Hall, P. A. (1993). Policy paradigms, social learning, and the state: the case of economic policymaking in Britain. *Comparative Politics*, *25*(3), 275-296.

Hayne, C., & Free, C. (2014). Hybridized professional groups and institutional work: COSO and the rise of enterprise risk management. *Accounting, Organizations and Society*, *39*(5), 309-330.

Her Majesty's Treasury. (2014). *The orange book: management of risk – principles and concepts*. Retrieved from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/220647/orange_book.pdf

Huber, C., & Scheytt, T. (2013). The dispositif of risk management: reconstructing risk management after the financial crisis. *Management Accounting Research*, *24*(2), 88-99.

Instrução Normativa CGU n. 03, de 9 de junho de 2017. (2017). Aprova o Referencial Técnico da Atividade de Auditoria Interna Governamental do Poder Executivo Federal. Retrieved from: https://www.cgu.gov.br/sobre/legislacao/instrucoes-normativas

Instrução Normativa Conjunta MP/CGU n. 1, de 10 de maio de 2016. (2016). Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal. Retrieved from: *https://www.cgu.gov.br/sobre/legislacao/arquivos/instrucoes-normativas/in_cgu_mpog_01_2016.pdf*

International Organization for Standardization. (2009). *Risk management: principles and guidelines* (31000:2009). Geneva: Author.

International Organization of Supreme Audit Institutions. (2007). *Guidelines for internal control standards for the public sector: further information on entity risk management* (INTOSAI GOV 9130). Brussels, Belgium: Author.

Jackson, A., & Lapsley, I. (2003). The diffusion of accounting practices in the new "managerial" public sector. *International Journal of Public Sector Management*, *16*(5), 359-372.

Lei n. 13.303, de 30 de junho de 2016. (2016). Dispõe sobre o estatuto jurídico da empresa pública, da sociedade de economia mista e de suas subsidiárias, no âmbito da União, dos Estados, do Distrito Federal e dos Municípios. Brasília, DF.

Lei Complementar n. 101, de 4 de maio de 2000. (2000). Estabelece normas de finanças públicas voltadas para a responsabilidade na gestão fiscal e dá outras providências. Brasília, DF.

Leitch, M. (2010). ISO 31000:2009 – the new international standard on risk management. *Risk Analysis*, *30*(6), 887-892.

Maijoor, S. (2000). The internal control explosion. *International Journal of Auditing*, *4*(1), 101-109.

Meyer, J. W., Boli, J., Thomas, G. M., & Ramirez, F. O. (1997). World society and the nation-State. *American Journal of Sociology*, *103*(1), 144-181.

Miller, E. A., & Banaszak-Holl, J. (2005). Cognitive and normative determinants of State policymaking behavior: lessons from the sociological institutionalism. *Publius*, *35*(2), 191-216.

Ministério do Planejamento, Desenvolvimento e Gestão. (2013). *Guia de orientação para o gerenciamento de riscos: versão final*. Retrieved from: http://www.gespublica.gov.br/sites/default/files/documentos/p_vii_risco_oportunidade.pdf

Moeller, R. R. (2011). *COSO enterprise risk management: establishing effective governance, risk, and compliance processes* (2nd ed.). Hoboken, NJ: John Wiley & Sons.

Organisation for Economic Cooperation and Development. (2012). *OECD integrity review of Brazil: managing risks for a cleaner public service* (OECD Public Governance Reviews). Paris, France: OECD Publishing.

Oulasvirta, L., & Anttiroiko, A. V. (2017). Adoption of comprehensive risk management in local government. *Local Government Studies*, *43*(3), 1-26.

Palermo, T. (2014). Accountability and expertise in public sector risk management: a case study. *Financial Accountability & Management*, *30*(3), 322-341.

Perez-Aleman, P. (2010). Collective learning in global diffusion: spreading quality standards in a developing country cluster. *Organization Science*, *22*(1), 173-189.

Rogers, E. M. (1995). *Diffusion of innovations* (4th ed.). New York, NY: The Free Press.

Scheytt, T., Soin, K., Sahlin-Andersson, K., & Power, M. (2006). Introduction: organizations, risk and regulation. *Journal of Management Studies*, *43*(6), 1331-1337.

Soule, S., & Earl, J. (2001). The enactment of State-level hate crime law in the United States: intrastate and interstate factors. *Sociological Perspectives*, *44*(3), 281-305.

Spano, A., Carta, D., & Mascia, P. (2009). The impact of introducing an ERP system on organizational processes and individual employees of an Italian regional government organization. *Public Management Review*, *11*(6), 791-809.

Standards Australia/Standards New Zealand. (2004). Australian/New Zealand Standard AS/NZS 4360:2004: *Risk Management*. Homebush, NSW: Standards Australia / Wellington: Standards New Zealand.

Strang, D., & Soule, S. A. (1998). Diffusion in organizations and social movements: from hybrid corn to poison pills. *Annual Review of Sociology*, *24*(1), 265-290.

Tribunal de Contas da União. (2009b). *Critérios gerais de controle interno na administração pública: um estudo dos modelos e das normas disciplinadoras em diversos países*. Brasília, DF: Author.

Tribunal de Contas da União. (2009a). *Portaria 189/2009.* Aprova a realização do projeto contas. Retrieved from: https://pesquisa.apps.tcu.gov.br/#/redireciona/ato-normativo/%22ATO-NORMATIVO-77379%22

Tribunal de Contas da União. (2012). *Acórdão 1.233/2012, Ata 19/2012 – Plenário*. Retrieved from: https://pesquisa.apps.tcu.gov.br/#/redireciona/acordao-completo/%22ACORDAO-COMPLETO-1233850%22

Tribunal de Contas da União. (2013). *Acórdão n. 7.128/2013, Ata 43 – Segunda Câmara*. Retrieved from: https://pesquisa.apps.tcu.gov.br/#/redireciona/acordao-completo/%22ACORDAO-COMPLETO-1295060%22

Tribunal de Contas da União. (2014). *Referencial básico de governança aplicável a órgãos e entidades da administração pública*. Brasília, DF: Author.

Tribunal de Contas da União. (2015a). *Acórdão n. 242/2015, Ata 5/2015 – Plenário.* Retrieved from: https://pesquisa.apps.tcu.gov.br/#/redireciona/acordao-completo/%22ACORDAO-COMPLETO-1371785%22

Tribunal de Contas da União. (2015b). *Acórdão n. 1.294/2015, Ata 19/2015 – Plenário.* Retrieved from: https://pesquisa.apps.tcu.gov.br/#/redireciona/acordao-completo/%22ACORDAO-COMPLETO-1420727%22

Tribunal de Contas da União. (2017a). *Referencial de combate à fraude e corrupção: aplicável a órgãos e entidades da Administração Pública*. Brasília, DF: Author.

Tribunal de Contas da União. (2017b). *Pesquisa integrada do TCU*. Retrieved from: http://portal.tcu.gov.br/inicio/index.htm

Tribunal de Contas da União. (2017c). *Acórdão n. 729/2017, Ata 12/2017 – Plenário.* Retrieved from: https://pesquisa.apps.tcu.gov.br/#/redireciona/acordao-completo/%22ACORDAO-COMPLETO-2251050%22

Troshani, I., Jerram, C., & Hill, S. R. (2011). Exploring the public sector adoption of HRIS. *Industrial Management and Data Systems*, *111*(3), 470-488.

Weyland, K. (2005). Theories of policy diffusion: lessons from Latin American pension reform. *World Politics*, *57*(2), 262-295.

Woods, M. (2009). A contingency theory perspective on the risk management control system within Birmingham City Council. *Management Accounting Research*, *20*(1), 69-81.

Zwaan, L., Stewart, J., & Subramaniam, N. (2011). Internal audit involvement in enterprise risk management. *Managerial Auditing Journal*, *26*(7), 586-604.

Flávio Sergio Rezende Nunes de Souza

https://orcid.org/0000-0001-6024-5200
Master's in Administration from the Foundation Getulio Vargas / Brazilian School of Public and Business Administration (FGV EBAPE); Cabinet of Institutional Security of the President of the Republic (GSI-PR). E-mail: flavio.nunes@marinha.mil.br

Marcus Vinícius de Azevedo Braga

https://orcid.org/0000-0002-7399-0952 PhD in Public, Strategic and Development Policy from the Federal University of Rio de Janeiro (UFRJ); Master's in Education from the University of Brasília (UnB); Federal Comptroller General's Office (CGU). E-mail: marcusbragaprofessor@gmail.com

Armando Santos Moreira da Cunha

https://orcid.org/0000-0002-3412-4031
PhD in Management from the Higher Institute of Work and Business (Portugal); Master's in Public Administration from the University of Southern California (USC); Professor at the Foundation Getulio Vargas / Brazilian School of Public and Business Administration (FGV EBAPE). E-mail: armando.cunha@fgv.br

Patrick Del Bosco de Sales

https://orcid.org/0000-0001-9204-8770
Master's in Administration from the Foundation Getulio Vargas / Brazilian School of Public and Business Administration (FGV EBAPE); Instructor at the Admiral Newton Braga Center of Instruction (CIANB). E-mail: del.bosco@marinha.mil.br