Audit Methodology Focused on Process and Risk

Antonio José Saraiva de Oliveira Júnior
is an auditor of the Federal Court of Accounts of Brazil, he has a BA in Economics from the University of Brasilia, specializing in Public Policy Analysis from the Getúlio Vargas Foundation (FGV).

Arnaldo Ribeiro Gomes
is an auditor of the Federal Court of Accounts of Brazil, has a degree in Accounting from the University of Brasilia (UNB) and is Certified in Control Self-Assessment (CCSA®) by The Institute of Internal Auditors (IIA), USA.

Guilherme de Vasconcellos Machado
is an auditor of the Federal Court of Accounts of Brazil, has a degree in Mechatronics Engineering from the University of Brasilia - UNB.

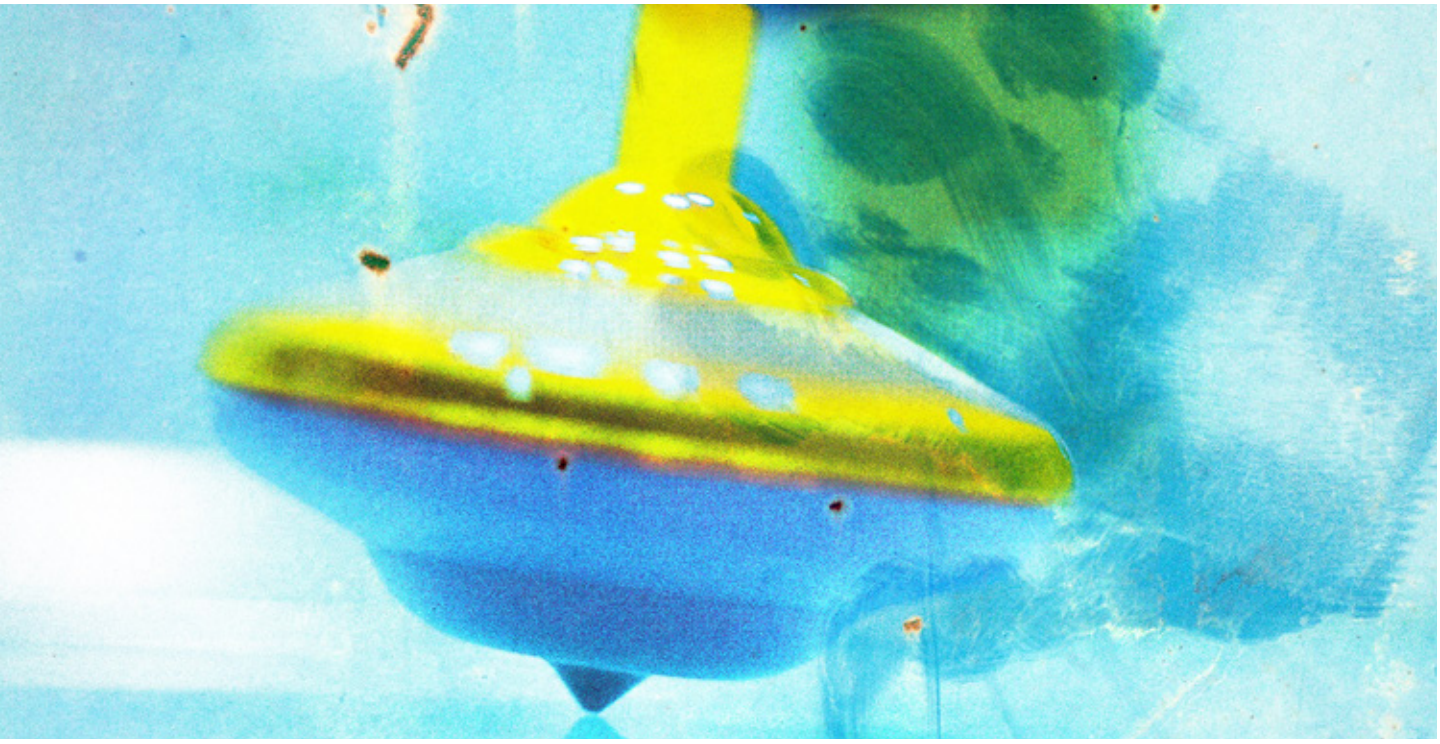
ABSTRACT

This article presents the general points of audit methodology aimed at the evaluation of risks and controls with focus on work processes, end activity or aid processes, which support the monitored object by means of the application of procedures and techniques to map out the processes involved, its objectives, risks and associated controls. The presented method possesses flexibility for the application in internal and external control audits and has the potential of contributing to the improvement of governance, regarding the component related to risk management and internal controls and, consequently, to achieve the objectives of the organization or of public policies.

Keywords: External Control. Public Governance. Audit Methodology. Risk Management. Internal Control.

1. THEORETICAL FOUNDATIONS

Risk management represents a continuing process conducted by the senior management, heads of departments and other employees, applied in establishing strategies formulated to identify, throughout the organization, events potentially capable of affecting it, and manage the risks in order to keep them compatible with the institution's appetite for risk



while providing reasonable assurance of achieving its goals (COSO, 2004).

Risk is the effect of uncertainty on the organization´s objectives (ABNT, 2009). It includes positive events with the potential to add value, and negative ones, with the ability to destroy value. The challenge facing the governance of organizations from the public sector is to determine how much risk they are willing to take in the search for the best value for the citizens and other stakeholders, which means providing services of public interest in the best way possible (BRASIL, 2014). The internal controls, however, are tools of the organization's risk management process and act in the mitigation of undesirable events.

It is in this context that an objective methodology is proposed, applicable to monitoring tasks of internal and external control of the Public Administration. As it is seen below, it is also applicable in private institutions without significant alterations, given the versatility of the auditing tools, although it is not the focus of this article.

The method presupposes the creation of risk matrices to evaluate the probabilities and impacts in relation to the stages of implementation of any management process, of which can be said to be large activity groups by which the organization fulfills its mission (BRASIL, 2013).

The core business processes are of big interest to the internal and external controls, since they refer to the essence of the organization, characterize its performance, are directly related to its strategic objectives and are supported by other internal processes, generating products and services for internal and external clients (BRASIL, 2013).

As a result of the application of techniques and procedures, we obtain a qualitative and quantitative assessment of the risk management of an organization or public policy. The differential of the methodology is the capacity of objectifying the results, as I will explain later.

In Brazil, there are few agencies or public institutions which have formally established risk management policies or practices. This gap makes the application of the methodology even more fruitful and educational, since it allows for pointing out the unconscious and informal risk management practices. Even if the institutions have not formally established risk management policies, they possess risk response elements (internal controls) that, when identified and evaluated, as proposed by the methodology, can be improved, thus contributing to the advancement of governance and the achievement of organizational objectives.

2. GENERAL AUDITING STANDARDS AND APPLIED CONCEPTS

The Auditing Standards of the Federal Court of Accounts of Brazil (TCU) – NAT (BRASIL, 2010) and the International Standards for the Professional Practice of In-

ternal Auditing (IIA, 2012) recommend the establishment of objectives for each audit work. According to these guidelines, a preliminary evaluation of objectives and relevant risks related to the audit object should be made, where the results should reflect the objectives established for the audit. In the development of the objectives one should consider, beyond the significant exposures to risk, the probability of errors, irregularities and breaches of principle, legal norms and applicable regulations.

In the planning phase, to determine the extent and scope of the audit, the auditor or audit unit should provide information on the objectives related to the subject being audited and the relevant risks associated with these objectives, as well as the reliability of controls to address the undesirable events.

When in the audit, if the information concerning the objectives, risks and controls of the audited object is not available, this information should be obtained in the planning phase of the work. The need and depth of the procedures for obtaining this data vary according to the objectives and the scope of the audit in question.

If the object and the scope of work are broad, the convenience of conducting prior and specific control action should be evaluated to obtain knowledge of the audited object, and its results should be considered in the planning and implementation of audit procedures focused on risks.

The proposed methodology enables the assessment of risks and controls and has the ERM model (Enterprise Risk Management) as a reference, from the Committee of Sponsoring Organizations of the Treadway Commission (COSO), a private organization established in the US in 1985 to avoid scams in financial statements of companies. The model considers that risk management institutions should be evaluated according to eight components (dimensions) that are intrinsic (COSO, 2004).

Along these lines, this methodology aims to evaluate the five core elements of the model, which can be translated into questions that pedagogically facilitate the understanding of the points:

a. **Setting Objectives:** has the unit set goals for the process or for public policy?

b. **Event Identification:** which events may present a risk to the objectives of the process or public policy?

c. **Risk Assessment:** what is the significance of the identified risks in terms of likelihood and impact of occurrence?

d. **Addressing the Risks**: has the organization implemented controls in response to the identified risks?

e. **Control Activities:** What is the quality of the established internal controls and to what extent do they ensure that the related risks will be mitigated to an acceptable level?

The choice of only five elements of the ERM model does not take away or reduce the importance of the others (control environment, information and communication, monitoring). Possible extension of the methodology allows the auditor to easily evaluate the other components of the model.

With respect to concepts applied to the methodology, one has the following:

- **Risk:** possibility of something happening and having an impact on the objectives of organizations, programs or government activities, being measured in terms of consequences and probabilities (BRAZIL, 2012a).

The risk event, therefore, materializes the risk, a negative consequence for the achievement of the institutional goals. In practice, the terms "risk event" and "risk" can be treated as synonyms.

- **Objective:** 'something' that was established to be achieved, of quantitative or qualitative character (BRAZIL, 2012b).

- **Internal control:** process fulfilled by management and the entire workforce, integrated into the management process in all areas and all levels of public agencies and entities, structured to address risks and provide reasonable assurance that, in achieving the mission, the objectives and institutional goals, the constitutional principles of public administration and the general control objectives are met (BRAZIL, 2012a). In short, internal controls represent a form of treatment (response) for risks, which are adopted to ensure, reasonably, that organizational goals are achieved.

Internal controls, therefore, represent governance tools available to managers, since they converge towards achieving the goals of the institutions and their programs.

- **Risk Source:** is the element that, individually or combined, has intrinsic potential to give rise to the risk and can be tangible or intangible (ABNT, 2009).

In other words, the sources of risk are all subjects, objects or situations that may cause a negative event. They are classified into six categories: people, processes, systems, infrastructure (physical or organizational) technology or even external events.

The risks are assessed in two dimensions, one before and one after the application of controls, as follows (BRAZIL, 2009):

- **Inherent risk:** the risk of the business, process or activity, regardless of the adopted administrative internal controls.

- **Residual risk** is the risk that remains after mitigation by internal controls.

Therefore, the residual risk is the inherent risk that remains after the implementation of administrative activities to reduce the probability and/or impact of the event in order to avoid, reduce, share or even accept the risk.

3. PROCEDURES

After understanding the basic conceptual framework, follows the exposure of procedures and techniques used in the construction of the scenario on the risk management of organizations and their sub-areas. The operational part is divided into four stages for better understanding.

3.1 IDENTIFICATION AND RECORD OF GOALS AND WORK PROCESSES (OVERVIEW)

At this stage, we must gather and understand the rules applicable to the object, the bylaws of the organization, previous work of internal and external control agencies on the subject, academic or technical articles, and other available information.

One should then identify the objectives of each activity and/or public policy to be audited as well as understand and record the stages of the work process that makes up the administrative activity, developed to achieve the established objectives. As an example, in the case of the process of decentralization of Union resources to other public or private entities through voluntary transfers of resources, one could divide the process into the following steps: a) reason for the transfer; b) selection of the decentralization recipient; a) conclusion of the adjustment; b) implementation monitoring; and c) analysis of accountability.

Then, to build detailed view of the object and the risk management, it should be required of the institution (i) information on strategic planning (or similar) and/or on the insertion of the audited in the strategic planning of the agency or unit; (ii) flow charts and narratives of the work process (textual description of activities); (iii) applicable internal regulations and relationship areas responsible for managing the object.

After passing the initial understanding phase of the audit, it goes to interviews with managers and operators of the processes or activities, in order to increase knowledge about the aims and implementation of activities in each step of the work process.

Meetings should be performed by applying interview techniques. In some cases, the team can deepen their vision of the object or confirm information through the review of process documents and related administrative acts. The obtained data should be used in the preparation of the following documents, which form the general view of the object:

a. **Flowchart:** document that provides a graphical representation of the work process, showing the sequence of activities, deadlines and the flow of documents between the areas involved.

It is noteworthy that the flowcharts should, as far as possible, be developed and, together with the responsible managers, adjusted and validated by date-stamping and signing, to avoid future questions.

b. **Narrative of the work process:** document describing, textually and with rich details, the sequence of management activities, legislation related to each step, the computer systems involved and the administrative control mechanisms adopted - standardized or just work practices performed by the sectors - responsible units, quantity and structure of staff, among other pertinent details.

Taken together, these documents provide ample understanding of the operation of the audited, especially its objectives, stages of the work process and activities

developed in them, thereby allowing the progress to the identification and risk assessment phase.

3.2 IDENTIFICATION AND ASSESSMENT OF RISKS

The third step comprises the identification of events that may affect the organizational goals established, and is associated with critical sense and professional judgment of the auditors, managers and operational staff responsible for the execution of the audited activity. This step must be a collective construction of the audit team based on the contributions of the managers and operators of the processes and, if possible, corroborated by other levels of internal or external audit. For identification and recording of risk events, one should make use of the Risk Matrix per Process. The structure will be exposed ahead.

In the matrix, which should already contain the objectives and stages of the work process, each member of the inspection team should identify, individually, the list of possible events that could negatively impact the achievement of the objectives of the audit, specifically based on the data obtained in the previous steps. The execution of such stage individually, at first, aims to enhance the private intellection of each member on any possibility of risk without interference or bias that may be generated by other team members.

After an individual survey, the team should meet to discuss the inventoried risks and especially possible others, by consolidating the results in a single matrix, moving then to the impact assessment (magnitude of a negative effect) and probability (estimate) of occurrence of each risk according to the variables of the following risk matrix. Whenever possible, there must be consensus on the team as to the existence and classification of the risks.

In support of the impact assessment and the risk probability and aiming to reduce the inherent subjectivity in the evaluation process, support tables should be developed containing qualitative criteria -

And where possible, quantitative - to assess the impact and probability variables (example: very high, high, medium, low and very low).

3.3 ASSOCIATION OF INTERNAL CONTROLS OF RISK AND CONTROL ASSESSMENT

At this stage, the auditor should identify the existing control mechanisms, correlating them to already cataloged risk events. Each risk should be associated with, if cases exist, formal and informal controls available to the unit which, directly or indirectly, can help to mitigate the identified risks.

An important activity in this step is to conduct workshops and/or additional interviews with managers and operators of the processes, in order to validate the inventoried risks and inquire about the internal controls associated with each risk. One must also consider the information about internal controls obtained in the initial phase of construction of the overview of the object. These meetings are also an opportunity for process owners to inform the staff about the existence of risks hitherto unidentified.

After identification and association of controls to the risks in the RMP, the quality of internal controls according to the evaluation categories established for the job (strong, satisfactory, moderate, weak or nonexistent) should be assessed both by the audit team

Table 1:
Risk Map
(probability vs. impact):

Risk Table						
		Probability				
		Very Low	Low	Medium	High	Very High
Impact	Very High	Medium 20	Elevated 40	Extremely high 60	Extremely high 80	Extremely high 100
	High	Medium 16	Elevated 32	Elevated 48	Extremely high 64	Extremely high 80
	Medium	Medium 12	Medium 24	Elevated 36	Elevated 48	Extremely high 60
	Low	Low 8	Medium 16	Medium 24	Elevated 32	Elevated 40
	Very Low	Low 4	Low 8	Medium 16	Medium 16	Medium 20

Source: MRP – SecexDesenvolvimento

Table 2:
Effects of the inherent risk mitigation in the internal controls

Control Evaluation	Mitigation	Obtaining the numerical value of the estimated residual risk
Non-existent	Estimated risk reduction of 4.5%	Multiply inherent risk by 0.95
Weak	Estimated risk reduction of 23%	Multiply inherent risk by 0,77
Moderate	Estimated risk reduction of 50%	Multiply inherent risk by 0,50
Satisfactory	Estimated risk reduction of 77%	Multiply inherent risk by 0,23
Strong	Estimated risk reduction of 95%	Multiply inherent risk by 0,05

Source: MRP – SecexDesenvolvimento

as well as the ones responsible for the process. In this case, questionnaires can be developed and applied to collect the views of the operational staff and management responsible for the process regarding the quality and/or control effectiveness in mitigating the risks.

At the evaluation of internal controls, qualitative scales should also be established and, if possible, quantitative, that contribute to reducing the inherent subjectivity in the evaluation process. In addition, for each category of evaluation, one should determine the effects control mechanisms will have on the inherent risks (whose valuation already considered probabilities and impacts), as follows.

Hence, the residual risk will portray the outcome of the formal or informal controls associated with each inherent risk event. The RMP, thus, displays information about the residual risk, based on the colors and values defined in the table used to assess the inherent risk (Table 1). The diagram below illustrates an example of a case study on the effect of control on the mitigation of inherent risk:

Therefore, from the application of the coefficients in the third column of Table 2 on the values associated with the risk of Table 1, it is possible to obtain an estimated numerical measure of the residual risk associated with each inherent risk, as the table below.

The estimated residual risk represents what is left of the inherent risk after the application of controls, or the portion of the risk that lacks internal controls to be mitigated fully. It is considered estimated because the effects of the controls have not been assessed at this stage of the work, in the case of estimation based on predominantly qualitative criteria (Table 2).

At the end of this step, you can define the extent and depth of the audit, based on the understanding of the objectives and implementation of the activity being monitored. The inherent and control risks are known and the design and quality of internal controls have been evaluated, obtaining as a result the residual risks of the process being audited. These references can be used to direct enforcement efforts in the evaluation of the key controls put in place to mitigate the significant risks (of higher probability and impact) to which the goal of the audited process is exposed.

3.4 SCOPING AND EXECUTION OF AUDIT FOCUSING ON RISK

From the understanding of the risks, the scope of the work should be set with a focus on process steps susceptible to events that may affect more severely in achieving the established objectives. The scope of the work can be limited to a particular step of the process, where the collective of risks of the selected step and monitoring resources warrant.

In the case of performance audit or survey - where the controls are not tested by procedures and

Figure 1:
Example of calculating the estimated effect of mitigation of the inherent risk by internal controls

Table 3:
Table of Residual Risk (inherent risk vs. control effectiveness):

Control Gap Table						
		Control Efficiency				
		Strong	Satisfactory	Medium	Weak	Non-existent
Risk Ranking	Extremely Elevated	Low 5	Medium 23	Elevated 50	Extremely Elevated 77	Extremely Elevated 96
	Extremely Elevated	Low 4	Medium 18	Elevated 40	Extremely Elevated 62	Extremely Elevated 76
	Extremely Elevated	Low 3	Medium 15	Elevated 32	Elevated 49	Extremely Elevated 64
	Extremely Elevated	Low 3	Medium 14	Elevated 30	Elevated 46	Extremely Elevated 60
	Elevated	Low 2	Medium 11	Medium 24	Elevated 37	Elevated 46
	Elevated	Low 2	Low 9	Medium 24	Elevated 31	Elevated 38

Source: MRP – SecexDesenvolvimento

auditing techniques – it is recommended to estimate the residual risks through workshops with process operators before the process. These meetings should provide for discussions with managers and/or the work process operators (crowded employees in units that deal daily with the management processes and are responsible for running them), in order to collect subsidies for the improvement of the assessments of risk events contained in the matrices, especially with respect to the probability, impact and procedures of internal control.

The meetings with the process operators, whenever possible, should be held without the participation of managers and no personal identification of those present, in order to allow greater freedom of expression. After closing the step of validation / contribution of the managers / operators of processes, the adjustments and reviews in the risk and control assessments should be made and the RMP completed in the final version.

The workshops are especially useful for the confirmation of the risk events pointed out at the RMP, through validation by the manager, of the possibility of materialization/occurrence of the negative event. Also serve to assess the existence and conformation of internal controls in response to risk events, or even the absence of these and the identification of new risks not yet detected by the inspection team.

On the other hand, when the risk assessment is a preliminary stage of a compliance audit (performed in planning), audit procedures should be modeled, during implementation, to assess the effectiveness of the controls associated with the risks included in the scope, making references to these procedures and their working papers in the specific field of RMP.

The definition of the scope of supervision should consider the situations of a lack or insufficiency of controls for significant risks as well as cases of unnecessary controls which result in an operating loss (inefficiency) for the process. It can also be proposed recommendations for the adoption of enhancement measures of internal controls.

After applying the procedures and auditing techniques to assess the effectiveness of internal controls (tests of controls) and having significant distortions regarding the risk assessment and/or controls initially recorded in the RMP, a review of this document should be performed.

3.5 SYSTEMATIZATION OF ANALYSIS RISK MATRIX FOR PROCESS (RMP)

The recording of qualitative and quantitative assessments should occur sequenced and associated with each risk event. Throughout each step of the identification process and evaluation of risk events, as well as evaluating the design of the controls, new information should be incorporated into the RMPs, an organized document that allows for integrated viewing and summary of the risk management elements catalogued throughout the work, based on the suggested following structure:

Each column must have the following information:

a. purpose of the agency / organization / program / activity audited;

b. stages of the audited process: teaching subdivision phases of administrative proceedings;

c. risks: inherent risks by process step, characterized by: risk event category (examples: operational, compliance, financial, information, image, etc.), classification of probability, classification of impact, assessment of the likelihood and impact assessment;

d. the result of inherent risk: numerical result of the inherent risk (multiply the probability by the impact, on a scale of 1 to 100, as shown in Table 2 as an example);

e. controls: description and classification (Strong, Satisfactory, Moderate, Weak or Non-existent) of the internal controls associated with each risk;

f. evaluation of the internal control;

g. result of the residual risk: numeric result of the estimated residual risk, in other words, the risk mitigated after the application of internal controls (ref Table 3, estimate);

h. reference to the internal control tests: reference to the audit procedures to evaluate the effectiveness of internal controls.

4. RESULT

At the end of the procedures, you get a structured view of the quality of risk management and internal controls of the audited object - one of the public governance components - with information on goals, work process steps and activities developed within it to achieve the goals, inherent risks associated with each step, adopted internal controls and its quality, as well as estimated residual risk in order to allow routing and optimization of audit efforts.

In addition, collaborative work of discussion with managers about the goals of the process under audit, risk and controls possess a high educational characteristic because it allows a deep reflection on the modus operandi of the units and of the activities developed, especially regarding ways to improve administrative internal controls.

5. APPLICATION IN TCU AUDITS

Regarding the audit types within the Federal Court of Accounts, the methodology can be used in surveys and audits. In the first case, you can cover a larger object, performing the first step in the planning phase and the next three in the implementation phase. The result perfectly converges for the purpose of the instrument, as stated in the TCU Survey Standards (BRAZIL, 2011), since it allows for the construction of the overview of the object and the risk assessment. In this case, the risk assessment extends to the evaluation of the estimated residual risk.

In compliance audits, it is possible to fully apply the same technique in the planning stage of the audit, as long as the scope is smaller. In this case, the result of the general risk assessment will elect the

Table 4:
Risk Matrix Structure by Processes (RMP)

		Risk	RI Evaluation	Controls	CI Evaluation	Residual risk:	CI Test Reference
Goal	step 1						PA - 1
							PA - 2
	step 2						PA - N
							PA - N
							PA - N
	step 3						PA - N
							PA - N
							PA - N

Source: MRP – SecexDesenvolvimento

main audit points and the feasibility of undertaking monitoring efforts on the subject. Once the scope is chosen and the object determined, control tests should be applied (procedures and audit techniques) to measure the actual residual risk.

6. CONCLUSION

Carrying out risk assessments and internal controls cannot achieve maximum effectiveness if objective techniques are not adopted and organized for this purpose. In order to meet this need is why this audit methodology focused on process and risk was developed.

In line with modern concepts of governance in the public sector, and meeting international standards of internal audit, as well as the audit standards of the Federal Court of Accounts of Brazil, the methodology consists of applying procedures in a systematic and organized way in order to map work processes by means of associating risks and control mechanisms.

In general, the construction of the scenario on risk management organizations is divided into four main steps: (i) identification and recording goals of the process to be audited (Overview): involves detailed knowledge of the object to be monitored and pieces are produced such as flow charts and narratives of the stages of monitored process; (ii) identification and risk assessment, addresses the identification, recognition and/or intellection of the possible events that could affect the objectives of the audit object, and is associated with critical sense and professional judgment of the auditors, managers and operators of the process under examination; (iii) Association of internal controls to the risks and evaluation of internal control: correlates control mechanisms to risk events; and (iv) Definition of the audit scope focused on risk: stage in which, from the knowledge built in the previous steps, you can set the scope of the audit to focus on significant risks, i.e. those whose materialization may cause greater impact to the detriment of achieving the objectives established for the audit.

The guidelines presented in this article serve as a guide for the auditor to, depending on his needs, deepen in the subject and start to apply the concepts herein in audit works, in order to contribute to the improvement of governance and hence for achievement of organizational objectives or policies.

REFERENCES

ABNT. Brazilian Association of Technical Standards. NBR ISO 31000: Risk management - Principles and guidelines, 2009. Available at: <http://www.abntcatalogo.com.br/norma.aspx?ID=57311>. Accessed: June 25, 2014.

BRASIL. Brazilian Federal Court of Accounts. Public Governance: Basic Governance Reference applicable to organs and entities of the Public Administration and Inducing Action Improvement. Brasilia: TCU, Secretary of Planning, Governance and Management, 2014.

_____. Brazilian Federal Court of Accounts. Decree No. 175/2013. It offers guidance to the jurisdictional units of the Court as to the development of content management reports for the year 2013. Brasilia, July 9, 2013.

_____. Brazilian Federal Court of Accounts. Glossary of Terms of External Control -. SEGECEX / Adsup / Adplan. Brasilia: TCU, September 2012a.

_____. Brazilian Federal Court of Accounts. Assessment Course of internal controls / Court of Audit.; Authors: Antonio Alves de Carvalho Neto, Bruno Medeiros Papariello. 2nd ed. - Brasilia: TCU, Serzedello Corrêa Institute, 2012b.

_____. Brazilian Federal Court of Accounts. Ordinance-SEGECEX-TCU No. 15/2011. Discipline on surveying and approving on a preliminary basis, the document Survey Standards. Brasilia, May 9, 2011.

_____. Brazilian Federal Court of Accounts. Annex to Executive Order No. 280/2010-TCU. Auditing Standards of the Federal Audit Court. Brasília, December 8, 2010.

_____. Brazilian Federal Court of Accounts. Eneral criteria for internal control in the Public Administration:. A study of the models and the disciplinary standards in different countries. Brasília, 2009. Available at: <http://portal2.tcu.gov.br/portal/pls/portal/docs/2056688.PDF>. Accessed: June 25, 2014.

COSO. Committee of Sponsoring Organizations of the Treadway Commission. Corporate Risk Management - Executive Summary, Framework and Risk Management in the Enterprise - Integrated Framework: Application Techniques, 2004. Portuguese version available at: <http://www.coso.org/documents/COSO_ERM_ExecutiveSummary_Portuguese.pdf>. Accessed: June 25, 2014.

IIA, The Institute of Internal Auditor. International Standards for the Professional Practice of Internal Auditing. São Paulo, 2012. Portuguese version available at: <http://www.iiabrasil.org.br/new/2013/downs/IPPF/standards2013_portuguese.pdf>. Accessed: June 25, 2014.