Proposal for implementation risk management according ABNT NBR ISO 31000 standard applied to internal audit process of Integrated Management System of IPEN

Wilson S. Scapin Jr., Tereza C. Salvetti and Guilherme C. Longo

Instituto de Pesquisas Energéticas e Nucleares (IPEN / CNEN - SP)
Coordenadoria da Qualidade – Diretoria de Planejamento e Gestão
Av. Professor Lineu Prestes 2242
05508-000 São Paulo, SP
wsscapin@ipen.br

Instituto de Pesquisas Energéticas e Nucleares (IPEN / CNEN - SP)
Coordenadoria da Qualidade – Diretoria de Planejamento e Gestão
Av. Professor Lineu Prestes 2242
05508-000 São Paulo, SP
salvetti@ipen.br

Reator Multipropósito Brasileiro (RMB)
Av. Professor Lineu Prestes 2242
05508-000 São Paulo, SP
glongo@ipen.br

ABSTRACT

The paper objective is to establish a risk management methodology applied to internal audits processes of IPEN Integrated Management System (IMS). In continuous seeking of updating methodologies to assist effective management based on the constant changes in the organizational world, and the development of management tools used for decision making, risk management demonstrates trends to be a new tool with high efficiency. This trend is accentuated by the fact that risk management is being incorporated into the new revision of quality management standard ISO 9001, estimated conclusion in November 2015. The identification, evaluation and treatment of risks are present in eleven items of its ten requirements at new revision. From the conclusion of the review, all organizations certified by that standard should make the necessary changes in their systems to meet the new requirements. This proposal will provide anticipate the changes that will occur in the management system of IPEN in accordance with this new revision. With the character of a pilot program to implement the organizational culture change in relationship to new concepts related to risks and implementation of risk management all other system processes that will be affected by the new revision of this standard. The methodology used for this paper is supported by the standards ABNT NBR ISO 31000.

1. INTRODUCTION

The Institute of Energetics and Nuclear Research - IPEN operates in research and development in nuclear and related fields, radioisotopes and radiopharmaceuticals production, provides irradiation services, tests and calibrations for industry, public and private organizations; develop human resources in nuclear and correlated fields. Finally, develop activities that respond to national interests and confirm the commitments made by the country regarding the peaceful use of nuclear technology.

By strategic reasons and to achieve their goals, IPEN maintains since 1999 a management system aligned with the standard ISO 9001 [1]. This standard is used as the basic framework to Integrated Management System (IMS) - IPEN make easier integration with other standards, supporting the Institute, among other demands, fulfillment of statutory and regulatory requirements for activities it performs.

One of tools to measure the performance of this system is the internal audits conducted regularly and on a scheduled basis to prove compliance of management system according the compulsory and voluntary standards.

The standards and regulatory requirements must be suited to the needs and demands that constantly changing according internal and external environments of organizations, so that must be reviewed and updated periodically. The Standard ISO 9001 since its first edition in 1987 has undergone several revisions. Currently the edition is 2008, however a new revision is in conclusion final stages, scheduled for November 2015.

The new review [2], presents significant changes in content will require efforts for organizations that use them to their full attention. Among the changes the new revision, there is concern about the identification and mitigation of risks. The concept of identifying and mitigating risks is the new revision of standard in eleven items of his ten requirements.

The Quality Coordination of Integrated Management System - IPEN, realizing that to upgrade all the IMS according the new revision requirements should implement considerable efforts, decided to anticipate part of this process. Like an embryonic process to begin adaptation to standard new revision requirements, it elaborated a risk management procedure according NBR ISO 31000 [3], applied to internal audit process approaching quality segment.

The purpose for this procedure is starting a dissemination of risk management concepts and opportunities for IPEN sectors directly involved with Integrated Management System. Also establish a positive environment to facilitate the paradigm change, very important for understanding the new management models. New management models are emerging with the dynamic changes by international scenarios due to new demands and technologies. The expectation is that from this initiative the necessary adjustments to meet the new revision of NBR ISO 9001 standard elapses effectively, optimizing resources (human, financial and structural) needed for this task.

While all organizations manage risk to some degree, the NBR ISO 31000 standard recommends that organizations develop, implement and continuously improve a framework whose purpose is to integrate the process for managing risks in governance, strategy and planning, management, reporting processes data and results, policies, values and culture throughout the organization.

When the framework for risk management is properly implemented, benefits can be expected such as:

- Increase the likelihood of achieving objectives;
- Encourage a proactive management;
- Attention for needs identify and treat risk throughout the organization needs;
- Improve identification of opportunities and threats;
- Compliance international standards and relevant legal and regulatory requirements;
- Improve the effectiveness of financial information;
- Improving governance;
- Improving stakeholder assurance;
- Establish a reliable basis for decision-making and planning;
- Improve controls;
- Provide and resources efficiently use for risks treatment;
- Improve the effectiveness and operational efficiency;
- Improve performance in health and safety as well as environmental protection;

- Improve loss prevention and incident management;
- Minimize losses;
- Improve organizational learning and
- Increase the organization resilience.

2. METOLOGY

To assess implementation feasibility of this methodology, possible difficulties and also to seek to illustrate the benefits can be reached, scenarios analysis requirements was performed using a SWOT analysis according, shown in Table 1 .

TABLE 1: SWOT Analysis

	OPPORTUNITIES (O)	**THREATS (T)**
EXTERNAL ENVIRONMENT	**1. Failure Reduction** • Improvement in the external image of the Institute with their customers , stakeholders and society; • Increased reliability of products offered. **2. Stakeholders relationships improvement:** • Motivation for the institution improves relationships with the stakeholders.	**1. Misalignment with customers and stakeholders :** • Because it is recent methodology cannot be recognized as it should. **2. Political Environment** • Changes in the political environment can affect the organizational structure and change the priorities of the institution
INTERNAL ENVIRONMENT	**1. Improving planning , performance and effectiveness:** • Opportunity to mitigate negative results and improve performance. **2. Economy and effectiveness:** • Effective use of resources; • Asset Protection; • Improved internal environment. **3. Improving information for decision making:** • Risk management provides information and more accurate analysis for decision making.	**1 – Resources availability:** **1.1 – Financial resources:** • Because it is public institution, the financial resources needed to eliminate or mitigation the risks may not be available as planned. **1.2 - Human resources:** • For the same reason above (1.1), the entry of new employers is rare and depends on public tender • Difficulty personal motivation for implementation a new management methodology.
	STRENGHTS (S)	**WEAKENESSES (W)**

The purpose of risk identification is develop a comprehensive list of risks sources and events that may impact objectives achievement (or key elements) identified in the contexts. ISO standards define RISK as the uncertainty effect on objectives.

The SWOT analysis showed implementation of a risk management process it would be appropriate to reduce future difficulties should appear for SGI- IPEN necessary changes in order to meet the requirements of the new revision of ISO 9001.

The methodology used for preparation of risk management procedures applied to the audit process followed the requirements established in IMS-IPEN internal Management Documentation procedures and guidance and guidelines established in the 19011 and 31010 ISO standards [4, 5].

Risk management can be applied in public or private organization, at a departmental level, for projects, individual activities or specific risks. Different tools and techniques may be appropriate in different contexts.
The ABNT NBR 19011 standard suggests in his item 5.3.4 that evaluate the risks that can affect the success of audits in at least six elements of this process:

Planning: for example, failure to establish the relevant objectives of the audit and determine the scope of the audit program;

Resources: such as allowing insufficient time to develop the audit program or conduct an audit;

Selection the audit team: for example, the team has the collective knowledge and competence to conduct audits effectively;

Implementation: for example, ineffective communication of the audit program;

Records and its controls: for example, failure to protect adequately the audit records to demonstrate the effectiveness of the audit program and

Monitoring, review and improvement the audit program: for example, ineffective monitoring of the results of the audit program.
The purpose of this work is developing a procedure for treating and or mitigation systemic way the risks mentioned above.

2.1 - AUDIT PROCESS

Different tools and techniques may be use for measure performance and effectiveness Management systems and so decisions can be more assertive. The most commonly used tools are: top management review, complaints and feedback from customers and stakeholders, performance indicators and internal or external audits.

Audits are planned evaluations, programmed and documented, conducted by expertise personnel and independent audited sector. The purpose of the audits is verifying the effectiveness of system by finding objective evidence and identification of non-conformities, like a feedback mechanism and improvement of the management system.
Internal audits are constituted as an effective tool for determining management system compliance levels of an organization in relationship to criteria (s) adopted (s) and provide valuable information for understanding, analysis and improvement to organization performance.The IMS- IPEN audit process is established taking the International Standard ABNT NBR 19011 recommendations and documented in the PG- IPN -1701 - Audit procedure.

2.2 PROCEDURE PREPARATION

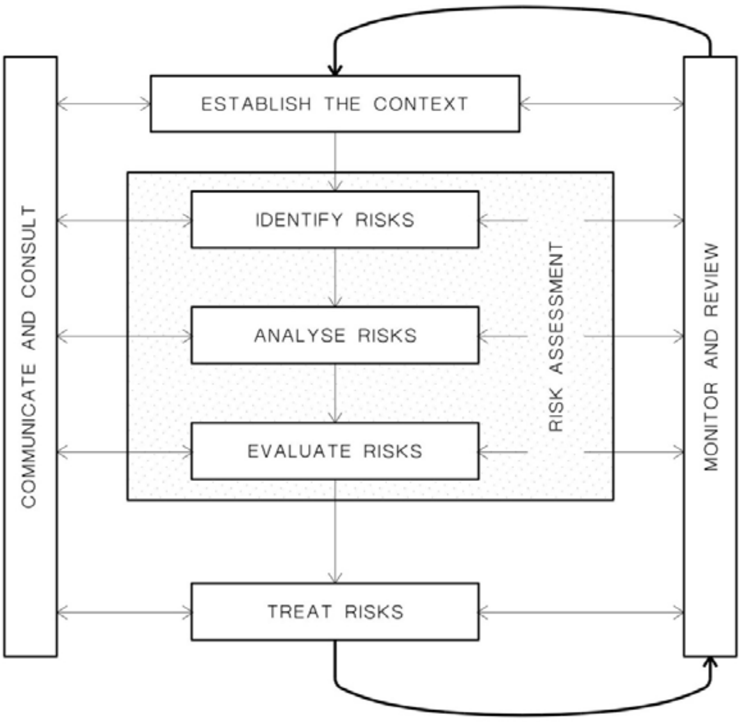
The procedure structure follows ISO 3100 Standard requirements described in **Figure 1** with subtle accommodation of specifics of process.

2.2.1 - Establishment the context

2.2.1.1 - External Environment: external environment which the organization seeks to achieve its objectives may include:

- The cultural environment, social, political, legal, regulatory, financial, technological, economic, natural and competitive;
- The key factors and trends that impact on the organization's objectives and
- Relationships with external stakeholders and their perceptions and values.

FIGURE 1: Risk management process – ABNT NBR ISO 31000



2.2.1.2 Internal Context: internal environment which organization seeks to achieve its objectives may include:

- Governance, organizational structure, roles and responsibilities;
- Policies, objectives and strategies implemented to achieve them;
- Ability understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);
- Information systems, information flows and decision -making processes (both formal and informal);
- Relationship with internal stakeholders and their perceptions and values;
- Organizational culture;
- Standards, guidelines and models adopted by the organization, and
- Form and extent of contractual relationships.

For audit process, the context was defined as being only factors associated with internal environment that may directly or indirectly be able to interfere in its performance.

2.2.2 Risk assessment process

2.2.2.1 Identify risks

• Identify what source of each risk;
• Identify what will be the objectives effect;
• Set when, where, why and how likely these risks (both positive and negative) occur;
• Identify who might be involved or be impacted;
• Check if there are currently controls to address this risk (maximize the positive risks or minimize the negative risks) and
• What could cause the control did not have the desired effect on the risk.

For the audit process risks identified were the six suggested according to ABNT NBR ISO 19011Standard:

- Planning;
- Resource;
- Audit team selection;
- Implementation;
- Records and controls and ,
- Monitoring, review and improvement of the audit program.

2.2.2.2 Risks analysis

Risk analysis involves consideration of the causes and its sources of identified risk, their consequences (C) and the probability (P) that those consequences can occur. Risk may be considered as a probability function (P) by the consequence (C):

$$\mathbf{R = P \times C} \qquad (1)$$

Risk analysis should determine quantitatively or qualitatively the probability and consequence of identified risks and through this relationship to establish a severity scale of these risks. For it was established:
• Describe identified risk;
• Determine identified risk cause and its source;
• Determine identified risk consequence (C).To determine the criticality of consequences inherent identified risks was prepared a table (table 2 - consequence Scale), within the context of audits to establish a severity level of gradation for these consequences.

TABLE 2 - Consequence scale (C)

Severity level	Descriptor	Definition
5	Catastrophic	Most objectivescan not be achieved
4	High	Some important objectivescan not be achieved
3	Moderate	Some objectives are affected
2	Minor	Minor effects that are easily remedied
1	Insignificant	Iinsignificant impact in goals

- Determine identified risk probability (P).To determine the probability occurrence identified risk was prepared a table (table 3 – Probability Scale), within the context of audits to establish a severity level of gradation for these probabilities.

• Determine the Inherent Risk level (IRL): product of probability (P) and consequence (C).

$$\mathbf{IRL = P \times C} \tag{2}$$

TABLE 3 - Probability scale (P)

Degree	Descriptor	Definition	Indicative frequency
5	Almost Sure	The event annually occur	Two times at year
4	Probable	The event likely occurred several times in their lifetime	One time at year
3	Possible	The event com be occur one time in their lifetime	Once every 02 years
2	Improbable	The event occur somewhere onde in a while	Once every 5 years
1	Rare	Is known that something similar occurred somewhere	Once every 7 years

2.2.2.3 Risk assessment to IRL answer definition

Definition for what do after determinate the inherent risk level (IRL) is called risk response. There are two situations for response to IRL:

a) Keeps the inherent risk: in this situation the IRL must be monitored so that it does not reach undesirable levels;

b) Treating the inherent risk: action that should eliminate or minimize the risk. They must be provided and monitored all the resources involved risk treatment.
For each risk identified and assessed as treatable should be only a single cause and a single consequence associated and thus the proposed treatments must be individual.

2.2.2.4 Risk response decision criteria

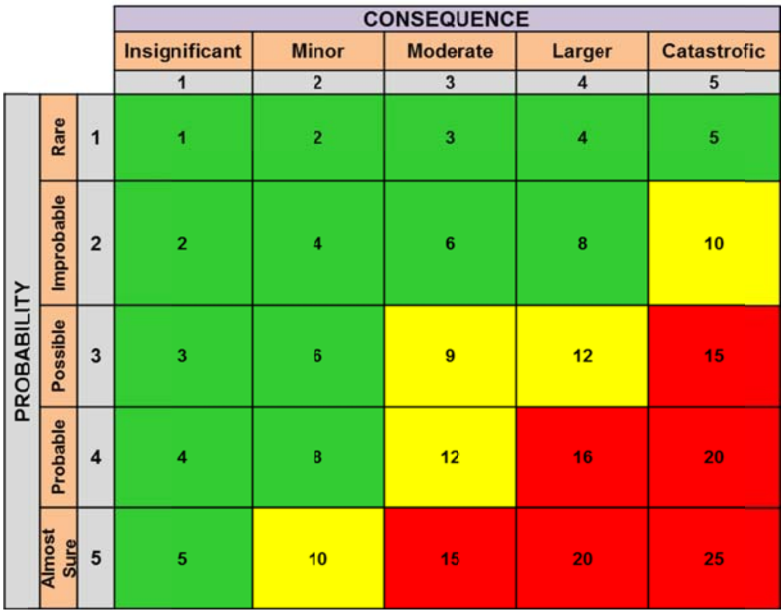
For IMS- IPEN has adopted the matrix Probability/Consequence (Figure 2 - Tolerability Matrix) and established the tracks to guide how best response to be adopted as follows:

•To IRY less than or equal 8, the risk may be accepted and monitored;

•To IRY greater than 12 the risk should be treated;

•To IRY between 9:12 the decision may be to accept or treat the risk. In case of acceptance, the risk should be monitored periodically. This region tolerability matrix is known as" ALARP" - (As Low As Reasonably Practicable), it means keeping the risks as low as reasonably acceptable and to achieve this level the IRY located in this matrix region should undergo a profound cost-benefit analysis for decisions taken.

FIGURE 2: Tolerability Matrix (probability x consequence)



			CONSEQUENCE				
			Insignificant	Minor	Moderate	Larger	Catastrofic
			1	2	3	4	5
PROBABILITY	Rare	1	1	2	3	4	5
	Improbable	2	2	4	6	8	10
	Possible	3	3	6	9	12	15
	Probable	4	4	8	12	16	20
	Almost Sure	5	5	10	15	20	25

2.2.2.5 Risks treatment

- Identification of alternative proposals and options to address the risk;
- Analyze and evaluate the necessary resources;
- Set the action and resources to treatment of risks;
- Prepare and implement the risk treatment plan;
- Analyze and evaluate the residual risks
- Establish which indicator will be used to monitor treatment of risk;
- Determine new probability (NP) for treated risk;
- Determine new consequence for treated risk (NC);
- Determine the Residual Risk Level (RRL): product of the new probability (NP) and new consequence (NC):

$$\mathbf{RRL = NP \ x \ NC} \qquad (3)$$

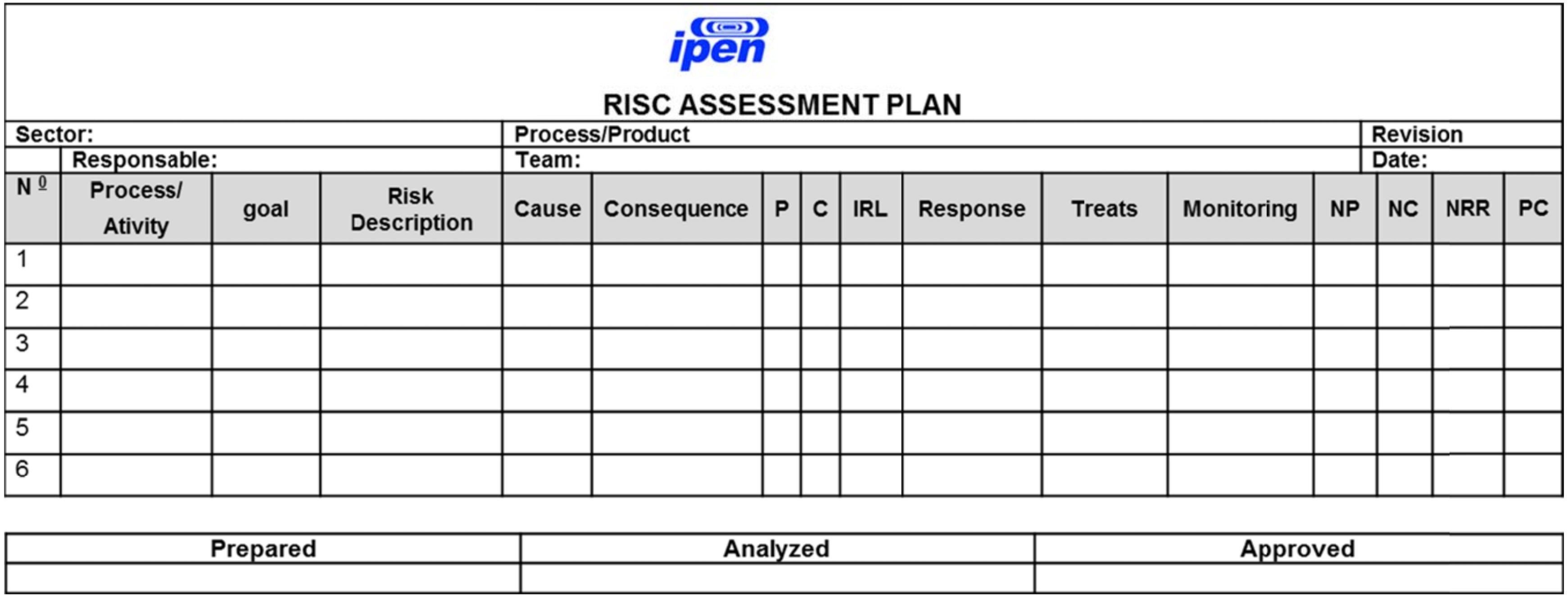
- Set the control point (CP)
- Set the period for the CP monitoring.

2.3 Risk Management

To risk management and treatment actions it created a datasheet (Figure 3 - Risk assessment plan) which are recorded all obtained indicators and processes, sectors and involved responsible.

The title of procedure is "IDENTIFICATION, ANALYSIS, EVALUATION AND TREATMENT OF RISKS" according IMS- IPEN documentation system. It was approved by direction in July 2014 and the risk assessment plan applied to audit process was concluded and approved on August 2014. As the procedure establishes a period of one year to review and / or analysis of plan, this step will be performed from August 2015.

FIGURE 3: RISK ASSESSMENT PLAN (datasheet)



RISC ASSESSMENT PLAN

Sector:	Process/Product	Revision
Responsable:	Team:	Date:

Nº	Process/ Ativity	goal	Risk Description	Cause	Consequence	P	C	IRL	Response	Treats	Monitoring	NP	NC	NRR	PC
1															
2															
3															
4															
5															
6															

Prepared	Analyzed	Approved

3. RESULTS AND DISCUSSION

The results of management risk applied to IMS-IPEN audit process is show above (table 4):

Risks identified:

a) Planning;
b) Resource;
c) Audit team selection;
d) Implementation;
e) Records and controls and
f) Monitoring, review and improvement of the audit program.

Objectives: for all identified risks the objective is the same; “Achieve the objectives of internal audits program 2014”.

For strategical institutional reasons the cause and consequence determination are not be showed.

TABLE 4 – Risks indicators

Risk	P	C	IRL	Response	Treats	Monitoring	NP	NC	NRR	PC
a	2	3	6	Maintain	monitoring	Top management and Audit process review	N/A	N/A	N/A	N/A
b	4	4	16	Treat	internal audit outsourcing	Top management and Audit process review	2	2	3	6
c	3	3	9	Maintain	monitoring	Audit process review	N/A	N/A	N/A	N/A
d	4	3	12	Treat	Encourage team members	Top management and Audit process review	2	2	3	6
d	1	5	5	Maintain	monitoring	Audit process review	N/A	N/A	N/A	6
f	2	2	4	Maintain	monitoring	Audit process review	N/A	N/A	N/A	6

NA-Not applicable

4. CONCLUSIONS

The procedure was concluded, approved and applied the audit process as planned. It was observed during preparation process and application procedure is that the biggest challenge is yet to come. With the release of the final revision of the ISO 9001 scheduled for November 2015, all other processes need adjustments to fit concept of risk management. New contexts should be established and probably the procedure for risk management has to be revised to coverage other SGI-IPEN processes.

The development of risk management plan applied to QMS-IPN internal audit process has been completed and the expectation of results is fruitful. Because it is implementing a new process, possibly there will be improvements and adaptations over time with the maturation of the concepts involved.

The proposals to identified, eliminate and/or mitigate risks will be reviewed for its effectiveness and suitability only from August 2015. For next internal audits IMS-IPEN in 2015, the expectation is that new risks can be incorporated into the risk management plan to ensure that the audit process remains protected in the best possible way to undesirable situations.

The methodology can be considered within the context of recent quality management systems, however, show strong indications of efficacy when applied correctly. It's a complex methodology is projecting its application to the various contexts that organizations are submitted.

An advantage has emphasized in this methodology, it´s the greater involvement of top management organizations for establishment risks treatments, eliminate or mitigate.

This involvement and commitment needs are associated with the resource factor for who makes decision as to its availability is the top management of organizations.

As a point considered sensitive, there is the complexity preparation of plans in all contexts involving organizations. The analysis of the relationship between cost and benefit, the ALARP region tolerability matrix, can cause risks requiring treatments end up being circumstantially deemed accepted.

5 – ACKNOWLEDGMENTS

Acknowledgment to Planning and Management Director - DGP-IPN Dr. Willy Hope who established trust and autonomy relationship to this paper could be carried out.

6 – REFERENCES

1. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, *Sistema de gestão de qualidade,* NBR ISO 9001, Rio de Janeiro, Brasil, 2008.
2. INTERNATIONA ORGANIZARION FOR STANDARDIZATION, *ISO/TC 176/SC 2/N 1147*, Vienna, Austria, 2013.
3. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, *Gestão de riscos – Princípios e diretrizes,* NBR ISO 31000, Rio de Janeiro, Brasil, 2009.
4. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, *Diretrizes para auditoria de sistemas de gestão* NBR ISO 19011, Rio de Janeiro, Brasil, 2012.
5. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *Gestão de riscos – Técnicas para o processo de avaliação de riscos*, NBR-ISO/IEC 31010, Rio de Janeiro, Brasil, 2012.