The 4 risks that weaken risk management

João Batista Ribas de Moura
Tax Analyst of the Federal Revenue of Brazil. Head of Internal Audit and Risk at the Administrative Council of Tax Appeals (CARF) of the Ministry of Finance. Master in Applied Computing. MBA in Strategic Management of Information Systems (FGV). Specialist in Management of Information Security and Communications (UnB)

ABSTRACT

Decree n. 9.203, of November 22, 2017, established principles, guidelines and mechanisms of governance at the direct, autarchic, and foundational federal public administration, and the risk management is essential to integrity and transparency, aspects which are essential for the administration. Despite all the theoretical and methodological consolidated benchmark, it has been observed that the practice of the process of risk management can be weakened due to risks that impact the full accomplishment and accuracy of the reports submitted to the controlling agencies and to the Brazilian society. This article aims at presenting the risks that jeopardize risk management and suggests preventive actions.

Keywords: Governance. Integrity. Risk management.

INTRODUCTION

Decree no. 9,203, of November 22, 2017, provides in its Article 4, Item VI, the guideline of 'implementing internal controls based on risk management, which will privilege strategic prevention actions before administrative proceedings'. Also in its Article 17:

> The senior management of organizations of direct, autarchic, and foundational federal public administration shall establish, maintain, monitor and improve risk management and internal control systems aiming at the **identification, evaluation, treatment, monitoring, and critical analysis** of risks that may impact the implementation of the strategy and achievement of the organization's objectives when fulfilling their institutional mission […] (BRAZIL, 2017, our bold types)

There is a set of frameworks, standards, or implementation guides to assist in the functionality of risk management. Among them, we note the *Orange Book*: *Management of risk - Principles and Concepts,* of the United Kingdom; *Committee of Sponsoring Organizations* (COSO) and the *International Organization for Standardization* ISO 31000 translated in Brazil according to the norms of the Brazilian Association of Technical Standards (ABNT). Whereas COSO is traditionally

oriented towards financial institutions, International Standard ISO 31000:2018 suggests a structure that is applicable to the most diverse profiles and, therefore, is more suited to the plurality of public organizations. Therefore, this article explores the sources of risk that weaken management under the perspective of rule 31000.

This rule provides guidelines to manage risks that have already been used at government agencies, which implementation model is divided into well-defined stages, as shown in Figure 1.

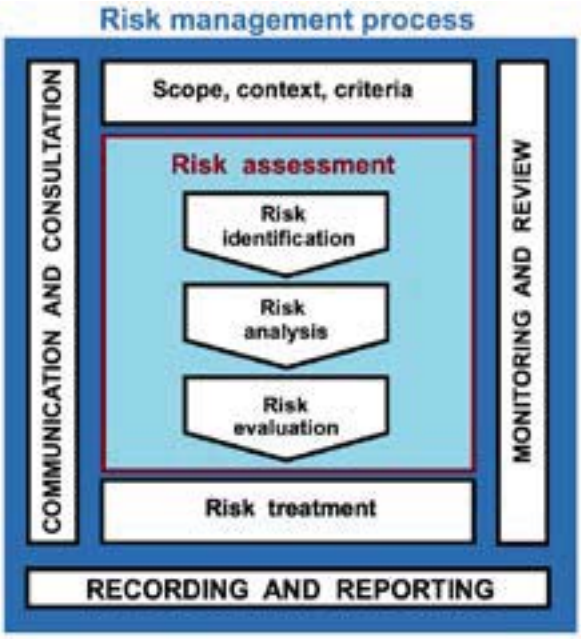

Figure 1: The risk management process.
Source Adapted from ABNT (2018)

Just as a construction, which, depends on a solid base obtained with quality materials, in order to be erected, the risk assessment process also depends on obtaining quality information at the initial stage of 'risk identification' to produce results that are truly useful to public managers. **The way in which several techniques concerning the recognition of risks is executed may lead to the production of incomplete or fraudulent reports.**

UNDERSTANDING RISK

The understanding of the concept of risk, though apparently trivial, often leads to erroneous strategies and rework when misinterpreted. The word 'risk' derives from the ancient Italian *risicare* and its meaning was to dare (BERSTEIN, 1997, pg. 8), in the sense of risk being an option and not a destiny whose events would depend on good or bad luck, without possibility of preventive actions.

The idea of risk has evolved with the statistics that allowed for the analysis of past events by calculating the probability of events recurring in the future under certain conditions. Thus, for example, if there is a background of a high quantity of robberies at a particular location and time in the city, it is possible to reduce the risk, or, in other words, reduce the probability of a

hazardous event occurring, by simply avoiding such area at those times. Therefore, it is not the case of predicting the future, but of scientifically analyzing the existing threats in relation to the vulnerabilities. Risk is not material or real, but a probability measure of something happening: when passing through an area with records of high rates of robbery at a certain time, for example, the 'risk of an incident is 90%'.

The two elements that constitute the **sources of risk** - threat and vulnerability (fragility) - can increase the chance of materialization of events - **consequence** - capable of jeopardizing the achievement of organizational strategic objectives.

> […] It is appropriate that risk should be described as the combination of the probability of an event (or danger **or source of risk**) and its **consequence.**
>
> The understanding that risk can have positive or negative consequences is a core and vital concept to be understood by the management. Risk may expose an organization to an opportunity as well as to a threat, or to both. (ABNT, 2015, pg. 8, our bold types)

The understanding that risk management strongly depends on the accuracy of risk identification, i.e., their vulnerabilities and threats, is essential for the successful outcome of the technique of collecting this information in the organizational environment. Normally, records of vulnerabilities receive greater detail than records of threats, since preventive or corrective actions can be more easily executed regarding the former. For example, the risk of skidding on rainy days can be reduced more easily by treating the vulnerability of bald tires rather than trying to reduce the threat of rain.

There are numerous techniques that can be used to identify risks. Many of these are described in the ISO/IEC ABNT Rule 31,010. Various organizations work with brainstorming, an activity where people are invited to report in groups, or fill out forms with the fragilities - normally internal - and threats - normally external - which they believe to be related to their work environments or processes into which they are inserted.

Many fragilities existing in the organizations are known only by the people who have worked there for years. They would hardly appear by using statistical techniques. This knowledge or wisdom, which is stored only in the minds of these people, is called **tacit knowledge** and needs to be transformed into **explicit knowledge** in order to be useful to management. Making explicit or documenting fragilities that lead to risks is the most valuable raw material, since it documents individual perceptions of the 'wrong things' existing in public organizations. The process of transforming this knowledge is outlined in Figure 2.

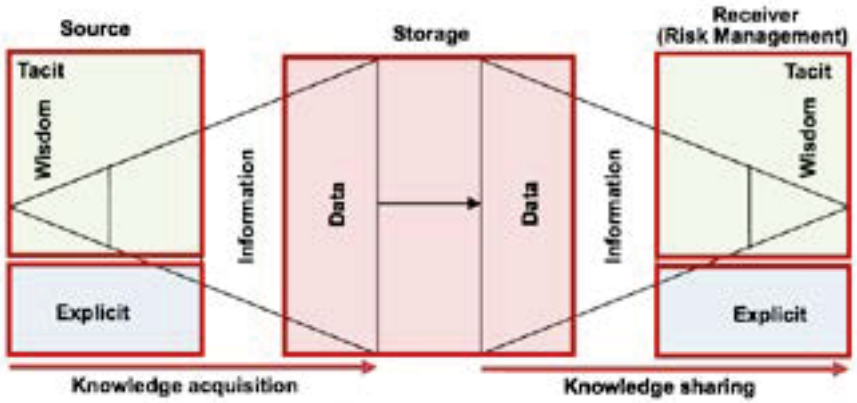

Figure 2: Transformation of tacit knowledge into explicit knowledge.
Source: Adapted from Kirsch, Hinem Maybury (2015, pg.66)

RISK AND INTEGRITY

Risk management should be used as a component of the integrity programs, since it has the power to reveal not only offenses previously categorized by legislation, but also other threats that are capable of jeopardizing the achievement of strategic objectives. Integrity is defined under Decree n. 9.203/2017 as one of the basic principles of public governance, and its relationship with risk assessment is shown in Figure 3.

Figure 3: Relationship between compliance, integrity and risk assessment.
Source Prepared by the author.

The term compliance is used to designate actions to mitigate risks and prevent corruption and fraud in organizations, regardless of the field of activity (SANTOS et al., 2012, pg. 1). In this sense, there is a continuous and worldwide effort of governments in the combat against corruption. The first anti-corruption compliance law emerged in the USA in 1977 and was called "Law on Corruption Practices Abroad (FCPA)". In 2011, the Bribery Act was approved in the

United Kingdom. In Brazil, several laws were created in this line:

- Law n. 7.492/1986 - Crimes against the National Financial System;
- Law n. 8.137/1990 - Crimes against the Taxation and Economic Order, and Consumption Relations;
- Law n. 8.429/1992 – Administrative Misconduct Law;
- Law n. 8.666/1993 - Procurement Law;
- Law n. 9.613/1998 - Crimes of Laundering or Concealment of Assets, Rights, and Values;
- Law n. 12.846/2013 - Anti-Corruption Law.

Integrity Program is defined under Administrative Rule n. 1,089, of April 25, 2018, of the Ministry of Transparency and Federal Office of the Comptroller-General (CGU), where guidelines for agencies and entities of the federal public administration are established:

> Article 2 For the purpose of this Administrative Rule, the following is considered:
>
> I - Integrity Program: a structured set of institutional measures concerning prevention, detection, penalty, and remediation of fraud and acts of corruption, in support of good governance; and
>
> II - Risks to integrity: risks that characterize actions or omissions that may encourage fraud or acts of corruption.
>
> […] (BRASIL, 2018).

In Figure 4 the **relationship between risk management and Integrity Program** is evident by the dependence of the latter in receiving from the former the list of risk events with a potential for materializing acts of corruption. Therefore, the possible actions that are damaging to the public treasury and that have not yet been detected in routine actions of control or audit - the integrity 'radar' - are unveiled by the ability that risk management has to bring to light sources of risk not yet made explicit in any organizational document.

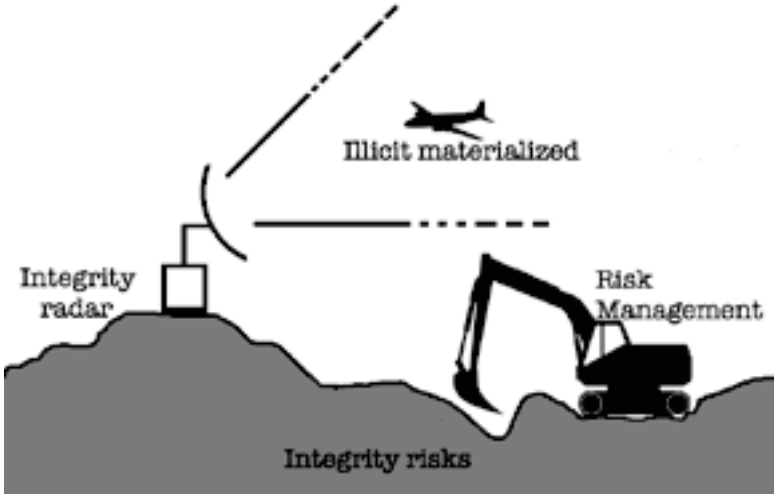

Figure 4: The integrity radar and risk management.
Source Prepared by the author.

RISKS TO RISK MANAGEMENT

As previously mentioned, the raw material for the risk assessment process is extracted at the identification stage, on which depend the subsequent stages of analysis, evaluation, and treatment. There is a set of sources of risks that renders their identification less efficient and contributes to **generating risks to their own management.** According to International Standard ISO 31000 (ABNT, 2018, pg. 2), 'source of risk is the element which, individually or combined, has the potential to originate the risk'.

The **first source of risk** arises when only bosses are heard in the identification process. Besides the natural tendency not to allow problems or fragilities existing under their responsibility to appear, the turnover in management posts leads them to not always know the details of their area of expertise as well as their subordinates do.

It suffices to open the Official Gazette any day in order to see the amount of commission posts that undergo dismissals and new appointments before, during, and after changes of government. The excessive managerial turnover not only destroys the value of the organization, but also goes against other ones. The efficient long-term relationships that were conquered are uprooted after the turnover, throughout the network of contacts, reducing loyalty, productivity, and destroying the value for the whole system. (REICHHELD; TEAL, 2001, p. 157).

In order to prevent this first factor from becoming a risk to management itself, it has been suggested that every 'factory floor' should be heard without any type of restriction, criticism or interference, since it is the great connoisseur of the vulnerabilities and threats existing in the labor activities.

The consequence of the use of of risk identification techniques that do not listen to all the subordinates, or which limit their participation, is the increase in the likelihood of risk management becoming incomplete and inefficient. Osborn (1963 apud Chapman, 2011, p. 175) is consistent with this thought when saying that during the exposure of ideas 'criticism should be discarded' and 'free thinking' encouraged.

The **second source of risk** stems from the use of a set of ready and closed-ended questions in forms or in interviews about the threats and vulnerabilities, which should be reported in the process of risk identification. Consequently, this reduces the organization's transparency for society, since it creates the possibility of incompleteness to the very process of risk assessment. Questions should not direct the thought of those who must pinpoint fragilities or failures. If, for example, when identifying the risks at a hangar, questions such as the following are put forward to the employees:

- Is the aircraft delivered revised and clean?
- Are the tires in good condition?

These questions direct the answers and do not allow freedom so that, for example, a mechanic is able to report the risk of a certain company often presenting their aircraft with fuel tanks almost empty after travel, indicating a probable nonconformity with the legislation that requires the maintenance of minimum levels of fuel to avoid incidents due to fuel exhaustion.

It is suggested that the **questions created for collecting tacit knowledge should be generic** (see Figure 2), not limiting the collaborators' responses, and should preferably follow a division of risks into categories (taxonomy) to stimulate thought in diverse areas where risks may arise: technology, people, budgeting and financial, operational, ethics, internal environmental, and external events. For Gupta (2016, pg. 5), it's essencial the understanding of the correctly identified sources of risk supported by a risk taxonomy that assists in measuring the impacts caused in case they materialize.

The **third source of risk** that jeopardizes the management itself arises where there is not enough support from the senior management, or when there are psychological sabotages in the form of open criticism to the work of risk identification. Resistance is expected during the implementation of any new procedure, since meetings, training sessions, completion of forms, or learning new systems require time previously destined for other activities. If bosses criticize the new procedures in front of their subordinates, thus discrediting the relevance of the work, those who hear these criticisms will not feel inclined to collaborate in identifying fragilities never exposed before.

For proactive reduction of this source of risk, it is suggested that senior management support the creation and maintenance of a culture of risk, where bosses and subordinates are made aware of the benefits that this management will bring for the improvement of the quality and safety of their own work environments. In this sense, Hillson (2016, p. 36) confirms that the real barriers to the implementation of risk management relate to people and not necessarily to the methodology or software. In relation to the senior management's frequent tone of support (top-down), **he also says 'more than empty words, it should be backed up by consistent and vigorous reinforcement actions'.**

The **fourth source of risk** may arise when the agency's risk management policy determines that the teams responsible for pinpointing the risks should also indicate solutions to mitigate them. In accordance with the Joint Normative Instruction n. 1 of May 10, 2016 (Brazil, 2016), the agencies and entities must institute risk management policies:

> […]
>
> Article 17. The risk management policy to be instituted by the agencies and entities of the Federal Executive, within twelve months from the publication of this Normative Instruction, shall specify at least:
>
> I - organizational principles and goals;
>
> II - guidelines on:
>
> how risk management will be integrated into the strategic planning, the
>
> processes and policies of the organization;
>
> (b) how and how often risks will be identified, evaluated, addressed, and monitored;
>
> (c) how risk management performance will be measured;
>
> (d) how the different levels of the agency or entity responsible for the risk management will be integrated;
>
> (e) the use of methodology and tools to support risk management; and
>
> (f) the continuous development of public agents in risk management;
>
> […]

The risk management policy is the first and foremost step towards the institutionalization of this management, since it offers support to the professionals that work in the area of risks to perform all the actions necessary to this management cycle.

Just as a *chef*, upon noticing the risk of a leakage from a tap, might not have the necessary skills to correctly assess the causes and the respective treatment of the risk, it is also likely that the servers of a public organization will not feel comfortable recording risks if they are jointly obliged to give guidance on the treatment of something beyond their expertise. This brings the damaging consequence to the process of identifying risks of omission in exposing the threats or vulnerabilities that generate them.

It is suggested that, during the creation or update of each public agency's or entity's risk policy, due **care should be taken to ensure that its wording does not discourage the process of risk identification,** i.e., that those responsible for identifying them are not automatically also made responsible for their correction, which, not rarely, requires multidisciplinary knowledge.

CONCLUSION

Risk management has become essential to public organizations due to its ability to identify threats and fragilities before they materialize into incidents capable of jeopardizing the achievement of strategic objectives, bringing damage to the public treasury and to Brazilian society. Despite all the recent legislation and every effort to put risk management and integrity programs into operation, there is margin for risks to management itself that bring a succession of damaging consequences: they reduce transparency, weaken integrity, and, forcibly, render governance less effective.

Management reports delivered to control agencies usually produce a generic vision of the risk management performance, without taking into consideration the details of the implementation of the identification process, a critical step to the management cycle, and from where the documented risks emerge. The four sources of risk that have been presented may be reduced by public management based on the suggestions outlined in this article.

Finally, future studies to create rules that guide to best practices of risk management operationalization can be a contribution to control agencies far beyond the analysis of content, but mainly to the way risk identification is performed as a major factor of reducing risks to their own management.

REFERENCES

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – **ABNT ISO/TR 31,004:** Gestão de riscos – Guia para implementação da ABNT NBR ISO 31.000, Rio de Janeiro, 2015.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – **ABNT NBR ISO 31.000:** Gestão de riscos – Diretrizes. 2. ed. Rio de Janeiro, 2018.

BERSTEIN, Peter L. **Desafio aos deuses:** a fascinante história do risco. 23. ed. Rio de Janeiro: Gulf Professional Publishing, 1997. 369 p.

BRAZIL. Decree n. 9,203, 22 nov. 2017. **Provides on the politics of governance of the direct, autarkical, foundational federal public administration.** Federal Official Gazette, Brasília, DF, Dec. 23. 2017. Section 1, p. 3.

_____ Normative Instruction n.1 of May 10. 2016. **Provides on internal controls, management of risk and governance in the context of the Federal Executive.** Official Gazette, Brasília, DF, n. 89, section I, pg. 14-17, May 11 . 2016.

_____ Administrative Rule n. 1,089, of April 25, 2018. **Establishes guidelines to ensure that the agencies and entities of the direct, autarkical, foundational federal public administration adopt procedures for structuring, executing and monitoring their integrity programs and other provisions.** Ministry of Transparency and Federal Comptroller General Office (CGU), Brasília, DF, 2018.

CHAPMAN, Robert J**. Simple Tools and Techniques for Management of risk Enterprise.** 2. ed. Croydon: John Wiley & Sons Ltd, 2011. 494 p.

GUPTA, Aparna. **Management of risk and Simulation.** New York: CRC Press, 2016. 523 p.

HILLSON, David. **The Risk Management Handbook:** A practical guide to managing the multiple dimensions of risk. Croydon: Kongan Page Publishers, 2016. 336 p.

KIRSCH, Philipp; HINE, Amelia; MAYBURY, Terry. A model for the implementation of industry-wide knowledge sharing to improve risk management practice. **Safety Science,** Amsterdam, vol. 80, p. 66-76, 2015.

REICHHELD, Frederick F.; TEAL, Thomas**. The loyalty effect:** the hidden force behind growth, profits, and lasting value. Boston: Harvard Business School Press, 2001. 323 p.

SANTOS, Renato Almeida dos; GUEVARA, Arnoldo José de Hoyos; AMORIM, Maria Cristina Sanches; FERRAZ-NETO, Ben Hur. **Compliance e liderança: a suscetibilidade dos líderes ao risco de corrupção nas organizações,** einstein (São Paulo), São Paulo, v. 10, n. 1, 10p., 2012.

Received in 15/01/2018

Approved in 17/05/2018