Theoretical framework for Risk management monitoring, review and improvement process of FLOSS applications using key risk indicators - KRI at a public agency

Marcelo Horacio Fortino, João Marcelo da Silva, Milvon Lopes dos Santos, Marcelo Ataíde Neto and Marcelo Mafra Leal

Department of Computer Science, University of Brasılia
Brasília, DF, 70910-900 Brasil

Abstract. In the last decade, and due to a number of factors, including budget constraints caused by the economic crisis and the promotion of Free and Open Source Software - FLOSS by the brazilian federal government, public bodies have been increasingly using FLOSS both to cover own operational needs and to offer new and varied services to citizens.
In this context, good governance rules suggest the establishment of the risk management process, which, in accordance with the ISO/IEC 27005 and ISO/IEC 31000 rules, broadly defines the context definition, analysis and risk assessment, risk management, communication, and critical risk monitoring and review of the organization's assets.
For the risk monitoring and review process, the COSO organization promotes the use of key risk indicators - KRI that help monitor alerts, changes in risk conditions, or new risks that may arise in the course of day to day operations.
This article aims to present the theoretical framework for Risk management monitoring, review and improvement process of FLOSS applications using key risk indicators - KRI at a public agency.

Keywords: KRI, FLOSS, COSO, ISO 27005, Open-Source Software, OSS, Risk Management

1 INTRODUCTION

In the last decade, and due to a number of factors, including budget constraints caused by the economic crisis and the promotion of Free and Open Source Software - FLOSS by the brazilian federal government[1], public bodies have been increasingly using FLOSS both to cover own operational needs and to offer new and varied services to citizens.

FLOSS has several advantages compared to proprietary software, for example, it avoids relying solely on a single vendor (vendor lock in), promotes savings

[1] Governo Eletrônico.https://www.governoeletronico.gov.br/sobre-o-programa/diretrizes

on license fees, and provides flexibility to make modifications and adaptations to the needs of the organization (WOODS et AL, 2005) [1].

But it is not immune to risks. In this context, good governance rules suggest the establishment of the risk management process, which, in accordance with the ISO/IEC 27005 [2] and ISO/IEC 31000 [3] rules, broadly defines the context definition, analysis and risk assessment, risk management, communication, and critical risk monitoring and review of the organization's assets.

On this latter process, the COSO[2] organization encourages the use of the Key Risk Indicators (KRIs) that help monitor alerts, changes in risk conditions, or new risks that may arise during the organization's activities [4].

This article aims to present the theoretical framework for Risk management monitoring, review and improvement process of FLOSS applications using key risk indicators - KRI at a public agency.

2 EXTERNAL CONTEXT

Public organizations must comply with laws and regulations emanating from the Federal Government and the states. Nowadays, in the public sector is essential to advance in the establishment of corporate governance that aligns the strategy of the business objectives to the day to day operations to reach the goals established in the programmed plans. In this context, risk management improves results by achieving efficiency and effectiveness in the performance of daily operations and programs.

According to the policy of Electronic Government of Brazil, the use of free software should be promoted whenever possible. Guideline number 3 says about it *"... must be prioritize solutions, programs and services based on free software that promote the optimization of resources and investments in information technology"*[3]

The decision is not only motivated by economic aspects, *"...but because of the possibilities it opens up in the field of production and circulation of knowledge, access to new technologies and the stimulation of software development in collaborative environments and the development of brasilian software."*

In the context of the federal government, the IT department of the agency is guided by SLTI Normative Instruction IN 04/2014 [5] and Normative Instruction IN 01/2016 jointly with the MP/CGU [6].

Article 13 of IN 04/2014 establishes that a Risk Analysis should be elaborated by the risk team identifying, measuring the probabilities of occurrence and severity, and the actions planned to reduce or eliminate risks. Finally, the team must define the contingency actions in case the events take place.

In IN 01/2016, Article 1 establishes that the agencies and entities of the Federal Executive Branch should adopt measures for the systematization of practices related to risk management, internal controls, and governance.

[2] COSO. `http://www.coso.org/`

[3] Governo Eletrônico. `https://www.governoeletronico.gov.br/sobre-o-programa/diretrizes`

3 RISK DEFINITION

According to the ISO/IEC Standard GUIDE 73: 2009 Risk Management - Vocabulary [7] the risk is *"an effect of uncertainty in the objectives"*, where *"an effect is a deviation from the expected Positive and/or negative"* and the uncertainty is *" the state, even if partial, of the deficiency of information related to an event, its understanding, its knowledge, its consequence or its probability."*

To define the risk criteria one must decide the *"nature and types of consequences to be included and how they will be measured, how probabilities are to be expressed, and how a level of risk will be determined."* (ISO/IEC 31010, 2011, page 23) [8]

A posteriori should be established when a risk needs treatment, whether it is acceptable and/or tolerable and the appetite (degree of uncertainty that an entity is willing to accept, expecting a reward - PMBOK, 311) [9] to the risk of the organization.

The ISO/IEC Guide 73 [7] defines the risk management process as *"the systematic application of policies, procedures and management practices for the activities of communication, consultation, establishment of the context, and the identification, analysis, evaluation, treatment, monitoring and critical risk analysis."*

The ISO/IEC 27005 [2] establishes that the information security risk management process *"consists of context establishment (Clause 7), risk assessment (Clause 8), risk treatment (Clause 9), risk acceptance (Clause 10), risk communication and consultation (Clause 11), and risk monitoring and review (Clause 12)."*

4 FLOSS SPECIFIC RISKS

According to the FFIEC Guidance [10] three types of risks can be established in FLOSS: strategic risks, legal risks and operational risks.

Strategic risks include the ability to customize software, compatibility and interoperability with other applications, available support, return on investment or TCO, and maturity. The latter includes security, time in the market and analysis of the community that develops it.

The legal risks are about the type of license and if you have guarantees.

Operational risks are the integrity of the source code, available documentation, and external application support.

The Black Duck company in its study *Open Source Security Audits* [11] similarly establishes (strategic) security risks, licensing risks (legal) and operational risks.

5 INTRODUCTION TO ISO/IEC 27005

ISO/IEC 27005 [2] Information technology - Security techniques - Information security risk management, presents the cycle of risk control in the organization.

It is in compliance with ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 31001, and the terminologies presented in ISO/IEC Guide 73, Risks - Vocabulary.

The Standard contains the description of the information security risk management process and its activities. The activities of the process begin with the activity of Context Establishement, followed by the Risk Assessment that contains the Identification, Analysis and Evaluation of Risks. The Analysis stage includes the processes of Risk Identification, and Risk Estimation.

The risk assessment is related to processes BAI01 - Manage programs and projects, BAI02 - Manage requirements definition and BAI05 - Manage organizational change enablement of the corporate governance framework COBIT 5 [12] developed by ISACA[4].

Then, the following steps will be carried out: Risk Management, Risk Acceptance, Risk Communication and consultation, and Risk Monitoring and Review. In the figure 5 we can observe the complete process.

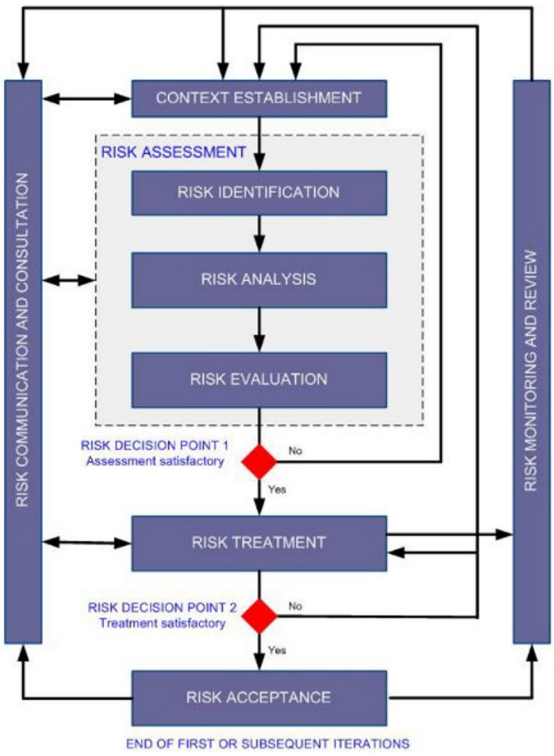

Fig. 1. ISO/IEC 27005. Font: ISO 27005:2011

[4] ISACA. `https://www.isaca.org/`

6 RISK MANAGEMENT PLAN CREATION

The agency established the creation of the Risk Management Plan to define, monitor and control the risks of the applications. Included in the plan are the methodology, functions and responsibilities, risk category, probability and risk impact definitions, risk tolerance level, format reports (how communications will be maintained, updated, analyzed and transmitted), and guidelines for monitoring, which are included in the Risk Monitoring and Control process.

This case study focuses on the definition of key risk indicators within the Risk Monitoring and Control process.

7 RISK MONITORING AND CONTROL PROCESS

The Risk Monitoring and Control process aims to:

- Monitor and control risks so that adequate response plans are implemented;
- Follow up on residual risks;
- Identify new risks; and
- Evaluate the effectiveness of risk management.

According to ISO/IEC 27005 [2], this process aims to critically analyze the Risk Management Process, identifying its needs, deficiencies and proficiencies.

This is a continuous effort, which must be carried out during all phases of the Risk Management Process, monitoring any changes in the organization context and the residual risks, so that they can be controlled. It also serves to consolidate the lessons learned and maintain an up-to-date risk overview.

The Standard ISO/IEC 31010 [8], states that it should be analyzed and verified that:

- The risk assumptions remain valid;
- The premises on which the risk assessment process is based, including the external and internal context, remain valid;
- Expected results are being achieved;
- The results of the risk assessment process are in line with current experience;
- The techniques of the risk assessment process are being applied appropriately; and
- Risk treatments are effective.

As a consequence, the agency defined that the responses and respective risk control measures previously established by the applications' managers will be monitored, with the purpose of evaluating the performance and effectiveness, through key risk indicators KRI - *key risk indicators* built for this purpose. The periodicity of the evaluations will be monthly.

8 COSO INITIATIVE

The COSO (Committee of Sponsoring Organizations of the Treadway Commission)[5] was created in 1985 in the USA in order to study factors that can lead to the generation of fraudulent reporting. The organization elaborates frameworks and recommendations for companies and their auditors in risk management, internal control and fraud detection.

In 1992 COSO launched the widespread framework COSO - Internal Control - Integrated Framework [13], which was last updated in 2013, being *"a conceptual model for the internal control system, useful for organizations in the development and maintenance of systems aligned with business objectives and adapted to the constant changes in the business environment."*(COSO, 2013).

COSO aims to standardize internal control definitions; define components, objectives and objects of internal control in an integrated model; outline roles and responsibilities of management; establish standards for implementation and validation; and finally create a means to monitor, evaluate and report internal controls.

In turn, the work Enterprise Risk Management—Integrated Framework [14], *"extends its reach into internal controls, offering a more vigorous and extensive focus on the broader subject of enterprise risk management."* (COSO, 2007).

The aim of that paper is to describe the essential components of corporate risk management, its principles and key concepts, along with the application techniques and examples related to each of the components, in order to facilitate its application.

For the definition of the key KRI indicators, it was based on the work "COSO Corporate Risk Management - Integrated Framework (ERM Framework)" [14]; and the article "Developing key risk indicators to strengthen enterprise risk management" [4].

9 KEY RISK INDICATORS - KPI

Several organizations are currently monitoring their progress with key KPIs - key performance indicators that track business goals.

The BSC - Balance Scorecard methodology, developed by Harvard Business School professors Robert Kaplan and David Norton, is generally used to provide the company with an integrated view because it encompasses indicators of financial performance, customers, internal processes, and learning and growth.

But these indicators do not present information about risk events that could hit the company because they are based on past events. As a result, COSO encourages the use of Key Risk Indicators (KRIs) that help monitor alerts, changes in risk conditions, or new risks that may arise in the course of day to day operations.

[5] COSO. `http://www.coso.org/`

It is important to note that the goal of developing effective key risk indicators is to identify relevant metrics that warn of potential risks that could have an impact on attainment objectives of the organization.

The key elements of well-designed Key Indicators should be: to be based on established practices or benchmarks, be developed throughout the organization, provide unambiguous and intuitive insight into monitored risk, facilitate measurable comparison between business units over time, provide opportunities to periodically verify the performance of risk owners, and consume resources efficiently [4]. (COSO, 2010. Page 6)

10 ESTABLISHING KRIs

In order to define the risks to be monitored and their respective controls, three specific risk indicators were defined for the monitoring of FLOSS applications using the *brainstorming* technique. In the formal session, IT managers participated along with the technical and business managers of the applications to be monitored.

The *brainstorming* technique aims to stimulate and encourage the exchange of ideas among a group of people to identify in this case the key risk indicators associated with FLOSS applications. *Brainstorming* can be formal or informal. The formal has a defined objective and is more structured, the informal is less structured and more free and personalized.

As a result, there has been established KRI for strategic risk and operational risks. The legal risk was disregarded in this case for monitoring through key risk indicators because it has a low degree of probability and impact.

For strategic risks, the two key risk indicators were: 1) The analysis of the application specific security forum, and 2) monitoring a general security forum, such as `https://nvd.nist.gov/`.

For operational risk instead, the two key risk indicators were: 1) monitoring the progress of the open issues and the relation between the open and closed ones with the purpose of conferring the degree of developer involvement in the application at the portal `https://www.github.com/`; and 2) the number of private companies that support the application.

In the figure 2 we present the key KRI risk indicators of FLOSS applications defined in the brainstorming session.

11 CONCLUSION

The great acceptance of FLOSS in public administration due to several factors, including single-vendor lock-in independence and savings in user licenses, it means managing the specific risks of these applications in such a way that the benefits of its use outweigh the possible problems arising from risks not monitored efficiently.

In this context, the use of key risk indicators becomes a viable and effective solution in the task of monitoring the risks of FLOSS applications. In the present

Source of risk - Cause	Event	KRI
Technological discontinuity	Lack of updates	Number of issues resolved in the last month https://www.github.com
Discovery security failure	*Hacker attack*	Vulnerability general and application's specific forums monitoring https://nvd.nist.gov
Lack of support	Discovery of bug or need for new functionality	Monitoring of suppliers on the IRS portal

Fig. 2. FLOSS KRI's. Font: M.H.Fortino

study case, this theoretical framework, using key risk indicators - KRI, was applied in the process of analysis and monitoring risks of the FLOSS applications of the IT department of a brasilian public agency.

In this study case, it was introduced the ISO/IEC 27005 [2] Information Security Risk Management standard definition of risk and the specific risks of FLOSS. In addition, there were enumerate the Risk Management Analysis and Monitoring Plan.

Afterwards, the COSO organization was presented, which, through the article *Developing key risk indicators to strengthen enterprise risk management* [4] recommends the Key Risk Indicators - KRI for monitoring risks. Finally there were defined the FLOSS applications KRIs for the agency.

As a result, we can affirm that the establishment of key risk indicators within the Risk Monitoring and Control process following the guidelines of ISO/IEC 27005 [2] and ISO/IEC 31000 [3] with the work Enterprise Risk Management - Integrated Framework [14] and the COSO organization article "Developing key risk indicators to strengthen enterprise risk management" [4]; facilitate the identification of errors, security issues, activity of the application developer community, and enable proactive action on risk management of FLOSS applications.

References

[1] Woods, D., Guliani, G.: Open Source for the Enterprise - Managing Risks, Reaping Rewards. O'Reilly, 2005.

[2] ABNT-ISO/IEC: ABNT NBR ISO 27005. ISO, 2011.

[3] ——: ABNT NBR ISO 31000 Gestão de Riscos. ISO, 2009.

[4] COSO: Developing key risk indicators to strengthen enterprise risk management, 2010. [Online]. Available: https://erm.ncsu.edu/az/erm/i/chan/library/coso-kri-paper-jan2011.pdf

[5] SLTI: Instrução Normativa (in04), 2014. [Online]. Available: https://www.governoeletronico.gov.br/
[6] MP/CGU: Instrução Normativa (in01), 2016. [Online]. Available: https://www.governoeletronico.gov.br/
[7] ISO/IEC: ISO Guide 73 Risk management Vocabulary. ISO, 2009.
[8] ABNT-ISO/IEC: NBR ISO/IEC 31010:2012, 2012. [Online]. Available: https://www.abntcatalogo.com.br/norma.aspx?id=89327/
[9] PMI: Um guia do conhecimento em gerenciamento de projetos (Guia PMBOK) Quinta Edição. Project Management Institute, Inc, Pennsylvania, EUA, 2013, vol. 2013.
[10] F. F. I. E. Council: Risk management of free and open source software, 2004. [Online]. Available: https://www.federalreserve.gov/boarddocs/srletters/2004/SR0417a1.pdf/
[11] Black Duck Software: Open source security audits, 2017. [Online]. Available: https://blog.blackducksoftware.com/top-three-operational-open-source-risks/
[12] ISACA: COBIT 5: Enabling Process. 2012. [Online]. Available: http://www.isaca.org/COBIT/Pages/Product-Family.aspx
[13] COSO: COSO - Controle Interno - Estrutura Integrada - Sumário Executivo, PWC, p. 20, 2013.
[14] ——: Gerenciamento de Riscos Corporativos - Estrutura Integrada, PWC, p. 135, 2007.