Enap Escola Nacional de Administração Pública

RSP

Enterprise Risk Management Agile Canvas: A Framework for Risk Management on Public Administration

Gustavo de Freitas Alves[1]
Mary Anne Fontenele Martins[2]
Rodrigo Lino de Brito[3]
Wildenildo Oliveira dos Santos[2]

[1]Hepta Tecnologia e Informática, Brasília, Brasil
[2]Agência Nacional de Vigilância Sanitária, Brasília, Brasil
[3]Ministério da Economia, Brasília, Brasil

Enterprise Risk Management (ERM) is a method of governance for managers as it offers a new point of view for monitoring and achieving an organization's objective. The ERM practices can be adapted to public organizations for strategic, tactical, and operational purposes. The focus of this article is to report the experience of developing and applying the ERM method to a regulatory agency through a case study. This locus research subject, the National Health Surveillance Agency (Anvisa), was chosen for its relevance in the context of the Brazilian public administration on risk management, due to its needs for internal controls and poorly developed risk maturity. This work has inductive reasoning and is characterized as an exploratory typology since there is little systematic and accumulated knowledge. The investigation deals with the Canvas model and its tools related to risk management – an emerging innovation framework that has readily been explored. The ERM Agile Canvas uses visual thinking allowing participants in workshops to contribute effectively with all stages established in national and international standards. It also enhances the risks classification and analysis by mapping and visualizing all of the Canvas and objectively planning ERM treatment. The method is adaptable and applicable to other public service organizations, in such a way that in a workshop one can apply techniques and work with several types of risks simultaneously. The results allow for a relationship comparison between sections, revealing the risk meaning and causality for improved public governance.

Keywords: Risk Management, Public Sector, Public Governance, Canvas

DOI: https://doi.org/10.21874/rsp.v71.i0.4363 ISSN: 0034-9240 | E-ISSN: 2357-8017
Submitted: February 12, 2020. Approved: November 17, 2020

Enterprise Risk Management Agile Canvas: um Framework para Gerenciamento de Riscos na Administração Pública

A Gestão de Riscos Corporativos (GRC) é um método de governança para os gerentes porque oferece um novo ponto de vista para monitorar e alcançar os objetivos organizacionais. As práticas de GRC podem ser adaptadas às organizações públicas em objetivos estratégicos, táticos e operacionais. O foco deste artigo é relatar a experiência do desenvolvimento de um método de GRC aplicada a uma agência reguladora por meio de um estudo de caso. O lócus de pesquisa, a Agência Nacional de Vigilância Sanitária (Anvisa), foi escolhido por sua relevância no contexto da administração pública brasileira de gerenciamento de riscos, devido a suas necessidades de controles internos e maturidade de risco pouco desenvolvida. Este trabalho tem um raciocínio indutivo e se caracteriza com uma tipologia exploratória, uma vez que há pouco conhecimento sistemático e acumulado sobre o assunto. A investigação trata de um modelo de Canvas e de suas ferramentas relacionadas ao gerenciamento de riscos, uma inovação ainda incipiente e, portanto, uma oportunidade a ser explorada. O Canvas Ágil de GRC usa o pensamento visual, permitindo que os participantes, concentrados em workshops, contribuam efetivamente, com todas as etapas estabelecidas nas normas nacionais e internacionais, na classificação e análise dos riscos, mapeando e visualizando o Canvas, e planejem objetivamente o tratamento de GRC. O método é adaptável ao serviço público, de tal modo que em um workshop pode-se aplicar técnicas e trabalhar com vários tipos de riscos simultaneamente. Os resultados permitem a comparação de relações entre as seções, revelando o sentido e a causalidade dos riscos para uma governança pública aprimorada.

Palavras-chaves: Gestão de riscos corporativos, Setor público, Governança Pública, Canvas

Enterprise Risk Management Agile Canvas: un marco para la gestión de riesgos en la administración pública

La Gestión de los Riesgos Institucionales (GRI) es un método de gobierno para los gerentes porque ofrece un nuevo punto de vista para monitorear y alcanzar los objetivos organizacionales. Las prácticas de GRI pueden adaptarse a las organizaciones públicas con fines estratégicos, tácticos y operativos. El objetivo de este artículo es informar la experiencia de desarrollar el método GRI aplicada a una agencia reguladora a través de un estudio de caso. Este objeto de investigación de locus, la Agencia Nacional de Vigilancia Sanitaria (Anvisa), fue elegido por su relevancia en el contexto de la administración pública brasileña de gestión de riesgos, debido a sus necesidades de controles internos y madurez de riesgo poco desarrollada. Este trabajo tiene un razonamiento inductivo y se caracteriza por ser una tipología exploratoria ya que hay poco conocimiento sistemático y acumulado. La investigación aborda el modelo Canvas y sus herramientas relacionadas con la gestión de riesgos, una innovación aún incipiente y, por lo tanto, una oportunidad para ser explorada. *GRI Agile Canvas* utiliza el pensamiento visual, lo que permite a los participantes, concentrados en talleres, contribuir de manera efectiva, con todas las etapas establecidas en los estándares nacionales e internacionales, a la clasificación y análisis de riesgos, mapeo y visualización de Canvas y planificación objetiva del tratamiento con ERM. El método es adaptable y aplicable al servicio público, de tal manera que en un taller puede aplicar técnicas y trabajar con varios tipos de riesgos simultáneamente. Los resultados permiten la comparación de las relaciones entre secciones, revelando el significado y la causalidad para la gobernanza pública.

Palabras-claves: Gestión de riesgos, Sector público, Gobernanza pública, Canvas

Introduction

Enterprise Risk Management (ERM) is an aiding method for managers providing a new point of view for monitoring and achieving organizational objectives. Some research support the ERM benefits (BROMILEY et al., 2015), while other studies suggest comparing cross-nationally risk governance to understand differences and what fits into the regulatory context (STEIN & WIEDEMANN, 2016)). Nonetheless, the risk management dimensions are not yet clearly defined, and the benefits for the organizations are not yet apparent ((HILLSON, 2016; POWER, 2004, 2009)). Public and private organizations need ERM to assess the risks affecting their objectives, but there is a great absence of ERM studies in the public sector concerning the practical application of ERM (CHANG et al., 2014; HANSSON, 2001).

The Brazilian Office of the Comptroller General – OCG and the Ministry of Economy – ME established guidelines present at the Normative Instruction 01/16, published on May 10th, 2016. They determined the adoption of Risk Management practices in the Federal Public Administration – FPA bodies and gave a deadline until May 10th, 2017 (BRASIL, 2016). The guidelines are related to the dissemination of ERM practices in the FPA to improve their control and to increase their effectiveness. The normative imposition is closely associated with the neo-institutional theory, which is concerned with the dissemination of practices among groups of similar organizations and contributes to the environmental influence investigation (DE.VRIES et al., 2016). While the normative imposition and theoretical background are widely discussed in academia, the practical application and objective's achievement of ERM implementation is a concern for public managers, who have to deal with compliance from higher superior bodies, such as the OCG.

Previous work has shown the lack of ERM studies in the Brazilian FPA (SANTOS et al., 2018), others trying to measure the Risk Management practices diffusion in the Public Sector (ALVES et al., 2017), how the risk management policy implementation is happening at specific public organizations (MARTINS et al., 2017), and the fit between Information Technology tools and ERM methods tailored to the FPA ((PAULO HENRIQUE DE SOUZA BERMEJO et al., 2019). With accumulated daily activities, lack of engagement or interest during the risk assessment, there is a practical gap of how the ERM can be

carried out by public servants, without it being burdensome, time consuming and unproductive.

As society benefits from public services, the Public Administration must deal with the risks to enhance the quantity and quality of services delivered to citizens, improving the country's development and welfare. ERM practices can be tailored to public organizations on strategic, tactical and operational objectives. Thus, the main question of this study is: How do ERM techniques and methods best apply to Anvisa, and possibly to other public organizations?

A practical contribution is to allow public managers to identify a pathway using the Canvas to enhance risk management internal control and improve organizational performance. Some related work developed a better visualization tool to address risk management communication (DONNELLY et al., 2012; EPPLER & AESCHIMANN, 2009), and this work seeks to develop good support on the risk management praxis connecting the ERM Framework and Canvas to the Anvisa's governance needs and sharing its experience with other public organizations for the operationalization of their risk management assessment.

It is also a continuation of previous work regarding Anvisa's Risk Management Policy development, which was a qualitative and descriptive exploratory study that aimed to report earlier experiences (MARTINS et al., 2017). With further advances in risk management implementation, Canvas emerged as an opportunity to systematically and intuitively deal with risk assessment.

1. Background

Will be presented in this section a background about modern theories of public governance and new public management, showing a rational approach for managing public sector risks will be presented. In sequence, the main enterprise risk management methods will be shown.

1.1. Public Governance and New Public Management

The growing diverse and complex social demands have led to the collapse of the State model as the sole provider of welfare. This reality has become more common since

the 1970s in several countries and, in this scenario, the prevailing consensus was that bureaucratic public administration, as a management paradigm, had become inadequate, slow, burdensome and inefficient. According to Denhardt and Catlaw (2015), '*the fiscal crisis of the 1970s resulted in various efforts to produce a government that works better and costs less*' (DENHARDT & CATLAW, 2015).

Given the multiple criticisms and that the managerialist prescription did not solve the problems of responsiveness and efficiency of public organizations, space was opened for a new management paradigm called Public Governance (POLLITT & BOUCKAERT, 2011). The idea of Public Governance gained strength at the end of the 1990s, in a context supplemented by pluralism, complexity, ambiguity and fragmentation of efforts – much of them provoked by unbridled initiatives and by managerial dialects from the New Public Management (POLLITT & BOUCKAERT, 2011).

The concept of Public Governance is sometimes used abstractly and subjected to different interpretations (DENHARDT & CATLAW, 2015). Public Governance seeks to emphasize that the traditional mechanisms of political management and control are no longer effective. For this reason, it makes no sense to talk about government without considering governance referring to the way that all sectors of society are involved and interact in the formulation and management of public policies.

Furthermore, risk management occupies an important place both in the New Public Management and Public Governance. Under the guidance of scientific management, there is a set of techniques recommended by the New Public Management, such as total quality management, service management, productivity compensation and risk management (ABRAHAMSON & EISENMAN, 2008). Nonetheless, the effects of 'managerial fads', typically associated with the New Public Management, imply the interest in risk management with a strong temporal correlation with the current organization's internal control needs (ABRAHAMSON, 1991).

From the perspective of Public Governance, recent literature offers a broader view on the value of risk management as one of the levels of quality and institutional capacity of a public organization, functioning as a mechanism to strengthen legitimacy, generate transparency and enable the increase of social control (MOORE, 2013).

1.2. Risk Management Methods

Enterprise Risk Management (ERM) is an ongoing process that consists of developing a set of actions aimed at controlling corporate risks capable of affecting the institution's objectives, programs, projects or work processes at the strategic, tactical and operational levels (COSO, 2004). The Committee of Sponsoring Organizations of the Treadway Commission (COSO®) issued the Enterprise Risk Management – Integrated Framework in 2004. Later, this framework was simply known as ERM Cube ® or COSO II ® (COSO, 2004). The new COSO version, published in 2017, is titled Enterprise Risk Management - Integrating with Strategy and Performance. In this new release, COSO sets out the key definitions, components, and principles for all levels of management involved in creating, implementing, and conducting enterprise risk management practices. In summary, this update: 1) adds greater insight into the value of enterprise risk management in defining and executing the strategy; 2) sets out the expectations of governance and greater transparency of stakeholders; 3) presents new ways of managing risk to establish and achieve objectives in the context of greater business complexity (COSO, 2017).

ISO 31000®: Risk Management – Principles and guidelines, define principles and guidelines in risk management, which can be adopted by different organizations in the activities of strategic decision, operation, process, function, project, service and risk assessment (ISO, 2009). In 2018 a new version of ISO 31000 was released, keeping most of its structure and supporting a practical approach for risk management (ISO, 2018). It can be applied to different types of risks, regardless of their nature, with a positive or negative impact. It does not imply the same risk treatment to different organizations – for that, one must evaluate the specificities of the organization. It should be used to harmonize the risk management process in existing and future standards by providing support, but not replacing these more specific standards. The standard is divided into principles, structure and process. Starting from a set of rules and guidelines, contained in the principles, the structure is then created to support the implementation of the risk management process in the organization, seeking out continuous improvement. The ISO process aims to establish the context, identify, analyze, evaluate and treat the risk, and communicate and monitor throughout the process (ISO, 2009, 2018).

The M_o_R® (Management of Risk) framework, developed by OGC®, is a guide designed to assist organizations in making decisions about risks that may affect the

achievement of strategic, program, project or operational objectives (OGC, 2010). It presents a method that addresses principles, approaches and processes in a set of interrelated steps using techniques and dimensions for risk management in organizations. There are notes and references for ISO 31000:2009® at the M_o_R framework; they are not competitors, but complementary to each other at the risk management praxis. As for dimensions, it covers them in details and presents information on the management of 1) business continuity; 2) crisis and incident; 3) health and safety; 4) information security risks; 5) financial risks; 6) environmental risks; 7) reputation risks; and 8) contract risks.

Risk management methods can help managers accomplish their organizational duties, but it is also necessary to understand these guidelines and how they are better tailored to different organizations. There is no "off-the-shelf" solution or framework that once adopted in any organization would perfectly deal with internal problems (DAMANPOUR et al., 2018). This way, in the context of Brazilian FPA, it is important to consider the best practices aforementioned, such as ISO 31000, M_o_R and ERM COSO, but also consider the local development and usage of tools and techniques tailored to the Brazilian culture and risk maturity level.

2. Method Locus and Focus

The focus of this article is to report an ERM framework tailored to the public sector through a case study, with qualitative and quantitative data, involving a specific situation of a contemporary phenomenon of ERM diffusion at Brazilian public organizations strengthened by a regulation recommendation called Joint Normative Instruction 01-2016 (BRASIL, 2016).

The present research object locus, the Brazilian Health Regulatory Agency (Anvisa), was chosen for its relevance within the Brazilian Public Administration context of risk management, because of its internal control needs and underdeveloped risk maturity.

This work has inductive reasoning and is characterized as an exploratory typology, since there is little systematic and accumulated knowledge regarding risk management practices in the public sector. The investigation deals with a Canvas model and its related tools for risk management, an innovation that is still being developed, and therefore, an opportunity to be explored.

Related to the bibliographical research, the framework was built following three stages: 1) free research; 2) framework and Canvas development with the detailed description, and 3) a literature review related to the best practice concepts and other study's results on risk methods.

3. ERM Framework development and Canvas usage

This section explains the ERM Framework and the description of each of its components, and the ERM Agile Canvas and all the steps to handle risks. Subsequently, it describes how to use Canvas, how to apply Canvas at Anvisa, and finally some findings on Canvas usage and its relationship with the ERM Framework.

3.1. The ERM Framework and its elements

Anvisa focused on prototyping a tailor-made method capable of joining the model of governance defined in its ERM policy, which is based on well-established methods such as ISO 31000, COSO ERM and M_o_R (Management of Risk) (COSO, 2004, 2017; ISO, 2009, 2018; OGC, 2010). A series of documents and structuring actions, coordinated in a set of interrelated steps, aimed at providing the organization with a standardized, inductive and result-oriented structure registered at Anvisa's Administrative Rule no. 854/2017, which defines ERM Policy, the establishment of the Risk Management Committee and the working process with the Risk Agents (BRASIL, 2017).

The Framework is cyclical, dynamic, and composed of elements at macro and micro level. It is structured on policies and documents for establishing ERM in Anvisa, according to Figure 1 (following clockwise).

The first macro document is the 'ERM Policy', defined as the organization's general statement of intent and direction for ERM.

To 'Define Risk Strategy' macro action, it is essential to understand that risks are subjective, and it is fundamental to establish criteria and prioritize which processes and programs are most critical to the institution, as well as to establish which approach will be adopted and how it will be implemented.

The following macro document is the 'ERM Process Guide', a step-by-step framework to be adopted in the whole organization. Moreover, the guide aligns the

understanding and language of ERM in the organization, defines activities, responsibilities and assures constant communication during the process.

The macro action followed is the 'Plan risks actions', a way of breaking down the risk subjectivity into something more tangible using criteria to support the risk analysis, which contains the identification, estimation and evaluation.

Next, another important macro document is the 'Communication Plan' which contains the guidelines on the communication mechanism, forms and periodicity of these notifications, covering both the strategic levels of top managers and going down to the operational level. To seek accurate and efficient communication, there should be no excess or lack of information, since such communications permeate decision-making.

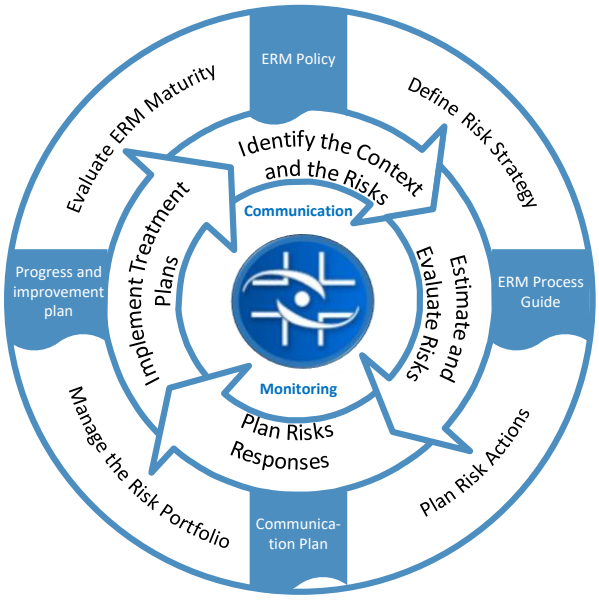
For the macro action 'Manage the Risk Portfolio' an ERM system was developed to centralize risk record information, enabling transparency and automated actions on the risk life cycle.

The macro document 'Progress and Improvement Plan' helps to build a path for evolution and the maturity level that Anvisa wishes to achieve on the next evaluation cycle. A set of structuring actions must be developed for each principle so that expectations are met.

Finally, the macro action 'Evaluate ERM Maturity' allows organizational reflection and understanding of its current capacity to plan and achieve improvements. Although there is no single solution for ERM development, the maturity assessment helps to define a path to be followed, allowing the incremental progress in short-term improvements and a long-term vision for the future. In addition, maturity measurement allows communication at an organizational level, sharing the objectives to be achieved, prioritizing actions to meet requirements, establishing a baseline and following up on its evolutions.

Figure 1 has the internal elements to carry out the management of specific risks – like the project, process, or any other organizational activities – and these are associated to a micro level, containing the classic stages of the ERM process: 1) Identify the context and the risks; 2) Estimate and evaluate risks; 3) Plan risks responses; 4) Implement treatment plans, and 5) Communicate and monitor.

Figure 1 - Anvisa's ERM Process

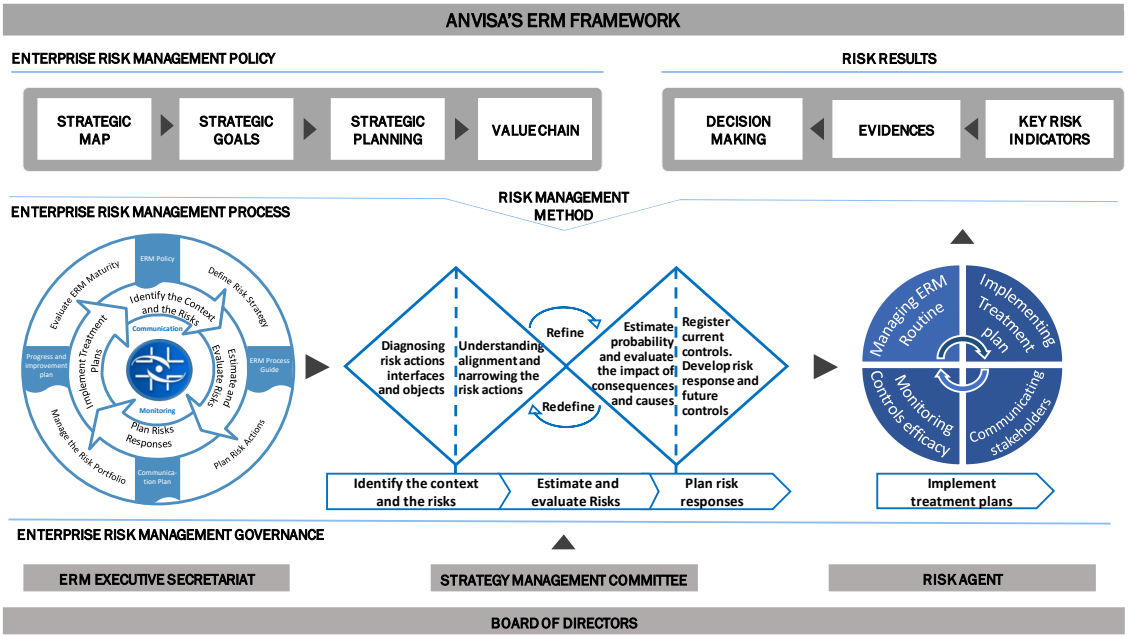


Source: Brasil (2018).

The Anvisa ERM framework was inspired by other frameworks such as ISO 31000, COSO ERM and Risk Management - M_o_R (COSO, 2004; ISO, 2009; OGC, 2010). The governance model binder to the Agency work process was the ERM policy and a set of interrelated steps aimed to provide a standardized structure focused on the agency results. Its milestones, actions and activities are represented in Figure 2.

The Anvisa ERM framework is aligned to the risk management policy and strategy management tools; guided by four macro documents: an ERM Policy, an ERM Process Guide, a Communication Plan; and a Progress and Improvement Plan. The four macro actions are: Define Risk strategy; Plan Risk Actions; Manage the Risk Portfolio, and Evaluate ERM Maturity. All macro documents and actions are materialized in five process stages: Identify the Context and Risks; Estimate and Evaluate Risks; Plan Risk Response; and a continuous and transversal process related to risks Communication and Monitoring for the stakeholders. The ERM Framework is focused on results, as 'Key Risk Indicators', 'Evidences' allowing 'Decision Making', supported by a governance model with defined roles and assignments.

Figure 2 - Anvisa's ERM Framework



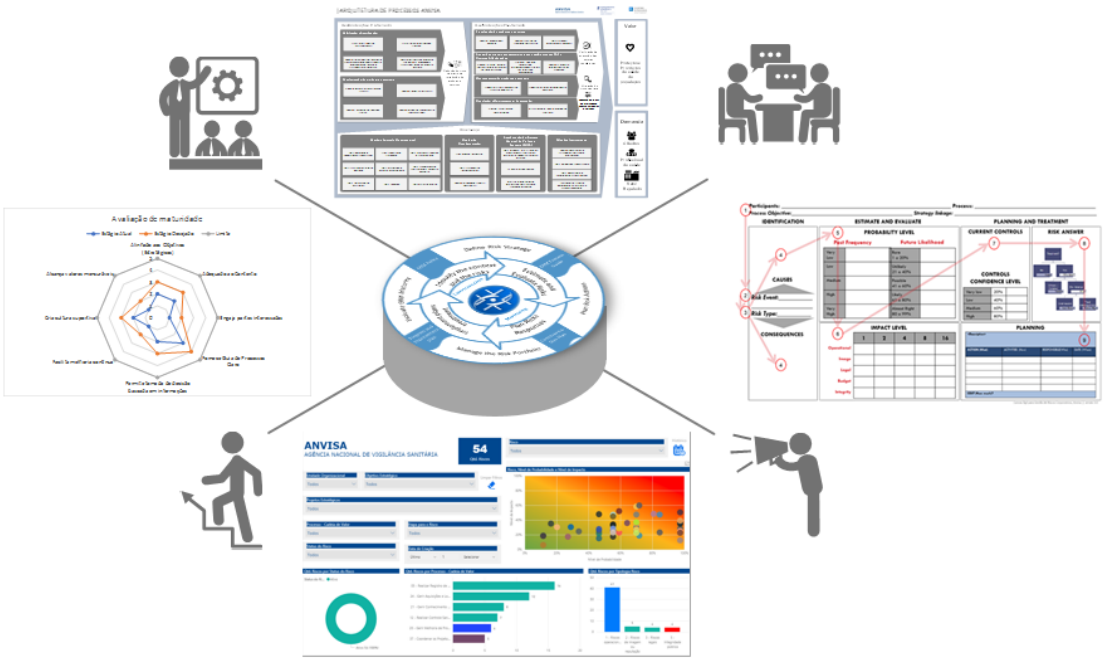
Source: Brasil (2018).

Regarding those roles, the 'ERM Executive Secretariat' is responsible for the whole ERM Process implementation based on the ERM Policy. The 'Strategy Management Committee' is the group responsible for issues concerning ERM responsibilities and other tasks related to: defining Anvisa's enterprise risk criteria; deliberating on the methods, procedures and practices inherent to the ERM; defining risk prioritization criteria and submitting recommendations and proposals to the Board; analyzing and presenting a critical analysis report to the Board; and assessing the adequacy, sufficiency, and effectiveness of the ERM process. The 'Risk Agents' are responsible for implementing the risk treatment plan and communicating and monitoring the risk over time. Finally, the 'Board of Directors' are responsible for approving the ERM policy and making strategic decisions based on the 'Evidences' and 'Key Risk Indicators' related to the 'Risk Results'.

Figure 3 shows a synthetic view of the method application and the suggested tools for each step. The ERM process brings together a set of interrelated tools aiming to deliver a more prescriptive method for risk management in the institution. Figure 2 synthesizes four structuring tools for building the framework: 1) Anvisa's Value Chain critical processes or other Strategic Planning action; 2) ERM Canvas as a supporting tool for the

risk discussion and its registry; 3) ERM System to manage the risk portfolio; and finally, 4) Risk maturity assessment tool.

Figure 3 - Anvisa's ERM Framework Tools



Source: Brasil (2018).

By using the framework's first tool, the high-level managers prepare for the ERM process at the organizational unit associated with the Value Chain critical process or the unit related to the Strategic Planning action. The managers and stakeholders must evaluate the internal and external environments, as well as the key factors that impact the achievement of the institutional objectives. Compliance and auditing reports are gathered, and other documents are made available for the risk specialists.

The documents are processed, and the risk events are raised for the workshop. Then, the second tool – the ERM Agile Canvas – is used to guide the meetings. The workshop output generates a Canvas for each risk event, and all information regarding the identification, evaluation, and planning for treatment is raised.

The ERM System records the Canvas output, allowing better communication and monitoring of each raised risk. The ERM System centralizes all risks, and then the executive summaries are developed by using its information.

Once a year, the maturity assessment is fulfilled. The form is based on M_o_R principles Health Check, and the results are calculated generating a historical baseline of ERM. This information enables the progress of risk management at the organization.

3.2. Enterprise Risk Management Agile Canvas

Agile methods improve communication and build trust among stakeholders, with the purpose of adding more value and developing institutional culture (BROWN, 2009). It is crucial to incorporate risk culture into actions, tasks and plans. To optimize the method application and the risk management process steps, the ERM Cycle and its dynamics were used in an Enterprise Risk Management Agile Canvas, a tool inspired by the Agile method and the Business Model Canvas ® management strategy, which allows us to make an easy and common language to the participants, thus, facilitating the shared understanding between the group (OSTERWALDER & PIGNEUR, 2010).

Visual thinking is characterized by using drawings and images to stimulate ideas or scenarios. The ERM Agile Canvas tool uses visual thinking, allowing the participants to quickly see the big picture and objectively plan the ERM treatment. The ERM Canvas allows the comparison of relationships between sections, uncovering the sensemaking and causality.

The main problems to be addressed with the ERM Canvas are related to: 1) The lack of engagement of managers, employees and risk specialists; 2) Difficulties on keeping the focus at the risk event; 3) Monopoly by active people vs. little involvement of the inactive, and 4) Slowness, bureaucratization and endless discussions.

Four differentials are present on the Canvas: 1) Visual thinking – the advantage that it can be represented by images and short texts instead of a long descriptive text; 2) Systemic view – once it allows visualizing the interaction between the nine sections; 3) Co-creation – since it enables participants of different levels, knowledge and experiences to contribute to the Canvas; and 4) Simplicity and applicability – because of its design and clarity it allows the model to be fulfilled and adjusted in less time (OSTERWALDER & PIGNEUR, 2010). Canvas helps in the development of risk perception for the strategy, processes and results obtained by the institution. It is a possibility to integrate knowledge and experiences with better information available and to visualize risks in a simple, integrated, direct and clever way.

This technique uses the ability to analyze risks through intuition, recognition of patterns, and development of new controls that are meaningful for the participants to predict risks in the near future.

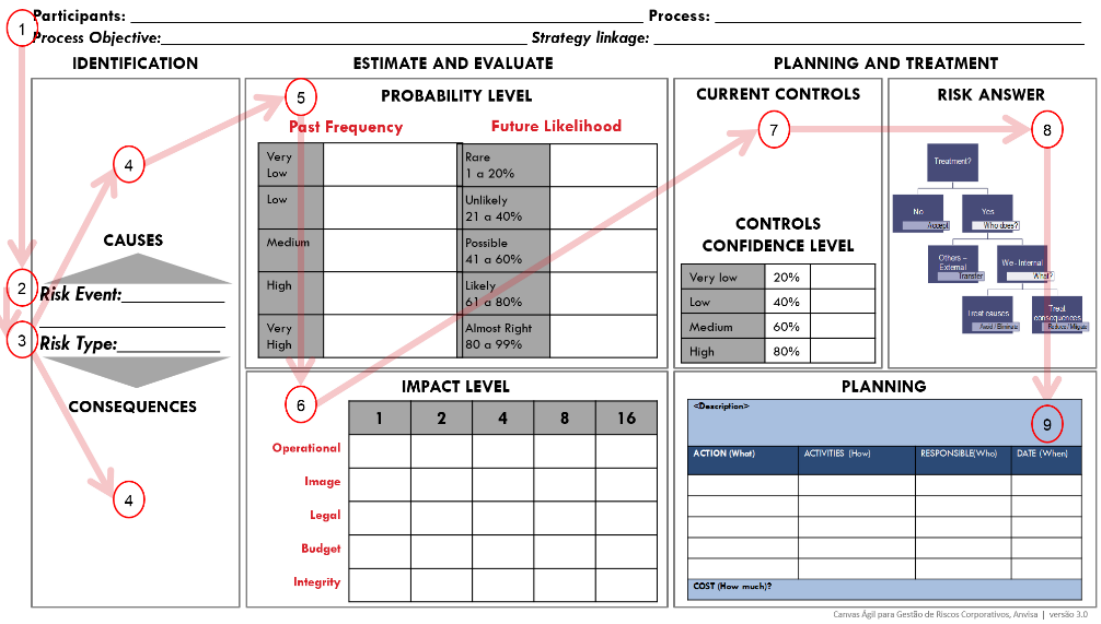
Some of the main reasons for using Design Thinking is due to the method's focus on people: Empathy – the ability to put yourself in the other's place is one of its essential elements; Collaboration – sharing ideas and perspectives for insights and actively involving not only managers but also other stakeholders in the process, as the owners of risk; and the use of divergent and convergent cycles of thought as a way of reflecting on contexts and situations, promoting the redefinition of causes and consequences of risks and controls.

3.3. How to use the Canvas

The workshop requires an interdisciplinary effort of people from different areas that must be applied to develop a holistic and systematic perspective of risk variables in each case. It is fundamental to apply the technique of design thinking for the practical use of Canvas, enabling creative and critical thinking to understand, visualize and describe the causes and consequences of risk events, as well as to obtain a practical approach for an effective resolution. Nevertheless, this framework offers tools aiding diverse strategic contexts to the participants, who need to think and apply these tools to a wide variety of risks, creating innovative and sustainable solutions for the institution (BROWN, 2009).

It is suggested to perform a pre-section work to compile the main risk events of an Organizational Unit to save time during the workshop. The context analysis and risk event steps are developed, and their results are consolidated and agreed upon with the risk owner – a specialist in the Value Chain process or Strategic Planning action. By understanding the risk context, it is possible to obtain enough information to initiate the workshop using the ERM Agile Canvas, registered in Figure 4.

Figure 4 - Enterprise Risk Management Agile Canvas



Source: Brasil (2018).

One Canvas is fulfilled for each risk event. The Canvas workshop begins with the definition of the Value Chain process to be analyzed, its objective and its association with the strategy are registered at the header. Next, the participants work on the main typology of the risk event (Integrity, Operational, Financial/Budget, Image or Legal). A timer is used during each step to control the group workflow with three different timebox. Once the risk event is reviewed by the group, during the first timebox, the definition of 'Causes' and 'Consequences' occurs by using a vertical bow-tie-like diagram. These causes and consequences are written on individual post-it notes and all groups take part in an evaluation round to contribute or adjust these notes in every Canvas.

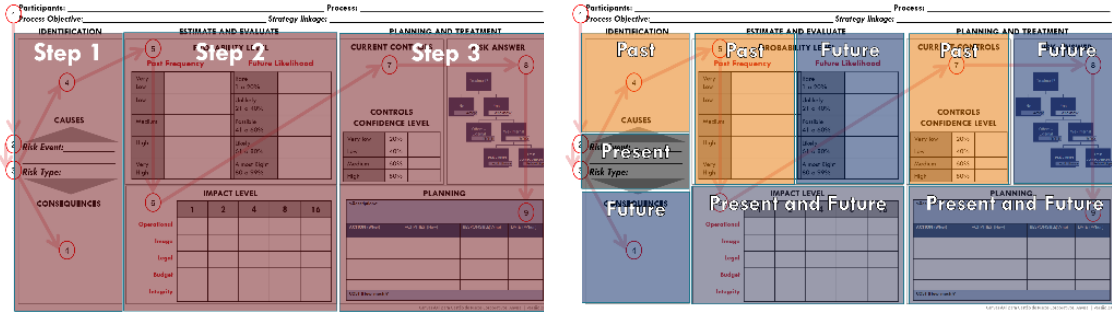
After the validation in the group, during the second timebox, the risk estimation begins by checking the probability analysis (Past frequency and Future Likelihood of occurrence) and the impact analysis (Using the five criteria listed in the typology), forming a Probability x Impact matrix. As there are still no historical series of risks, simple voting takes place at this stage, and each person should vote once and record their voting at the Canvas. During the sections, different colored shaped stickers were used to represent these votes. Impact analysis follows the same voting logic and people record their votes with stickers in the five impact typologies and scale levels for each criterion. For the impact analysis, it is recommended to use a supporting material containing an

exemplary list with the range of impact. A second evaluation round happens with each group validating every Canvas.

The third and last timebox begins. The type of risk response is chosen, followed by the survey of current controls and the confidence level these controls have. Depending on the response type, it is possible to elaborate on a treatment plan to deal with the causes or consequences listed in step 1. For the evaluation stage, the voting stickers are also used to determine the main type of treatment. A current control title is recorded in individual post-it notes. It is important to register these existing controls so that the participant does not plan the same control twice. This step creates visibility for the existing controls and allows better communication by the group. Finally, the 5W2H technique is used to carry out risk management planning. There is an association between evaluation and planning since the participants can focus on new solutions at the planning stage. Only the 'Accept' response type does not involve specific treatment planning.

As ERM presents itself with a perspective of anticipating the future before the risk event happens, the ERM Agile Canvas was built to optimize the ERM process at Anvisa. The Canvas is divided into three major steps: 'Identification', 'Estimate and Evaluate' and 'Planning and Treatment'. Each of these steps allows a reflection on the risk event to be dealt with and contains a timeline covering 'Past', 'Present' and 'Future', favoring an immersion in the discussions about the risk event, according to Figure 5.

Figure 5 - ERM Agile Canvas Steps and Timeframes



Source: Brasil (2018).

3.4. Workshops results

Throughout 2018 the Agency initiated the application of the ERM pilot projects at the following organizational units and their work processes:

1. Coordination of Strategic Programs of SUS (Single Health Service – *Serviço Único de Saúde*) – Sanitary Surveillance in Antimicrobial Resistance Action Plan;
2. Management of Cooperation and Partnerships – Anvisa Procurement process;
3. General Medicines and Biological Products Management – Medicines Registration and post-registration;
4. Planning Advisory – Strategy Management and Institutional Performance Process;
5. Planning Advisory – Improvement Management Process;
6. General Ports, Airports, Borders and Customs Enclosures Management – Issuance of Import License Proceeding;
7. Document and Corporate Memory Management – Document Management Process;
8. General Regulatory Management: Strategic Project nº 05 – Regulatory Process Improvement.

In the beginning, without the Canvas, the ERM was confusing and a lot of time was spent with the participants. After feedback of the ERM assessment of some units, the Canvas was developed. Canvas was first tested during the workshop held on April 23 to 27, 2018, which was attended by 22 representatives from Anvisa's Medicines Registration organizational unit. A second workshop was held in June 2018 with Anvisa's Ports and Airports organizational unit. The third workshop happened at the end of July 2018 with the Documental Management organizational unit. The last one happened at the end of August 2018 with the Planning Advisory Unit (Assessoria de Planejamento – APLAN) and was related to the Strategic Planning of Anvisa's objectives. All sessions served as inputs for recording risks on the ERM system and for further discussion on the risk treatment. It was observed that the Canvas guided the participants to see the 'big picture', saving time and engaged participants to finish the Canvas.

Before the workshop, during the auditing reports documental analysis, many risk perceptions were registered and clustered to develop a single risk event, and after those risk perceptions were suppressed. The risk event was set as the main discussion topic of one specific Canvas and the group contributed on this topic. Surprisingly, many risk perceptions reappeared during the development of the risk event causes and consequences, matching the suppressed risk perception and confirming them.

During the workshop, there were ties in some probability and/or impact level criteria. The tiebreaker for these items used the average and the rounding of the fractions.

Some of the workshop moments were registered in Figure 6.

Figure 6 - Workshop Sessions Results

Source: Authors.

The support of the working groups, representatives and managers were crucial for the workshop discussions. Few adjustments were made so that the framework, its definitions and tools were strongly connected to the proposed governance model.

3.5. Findings

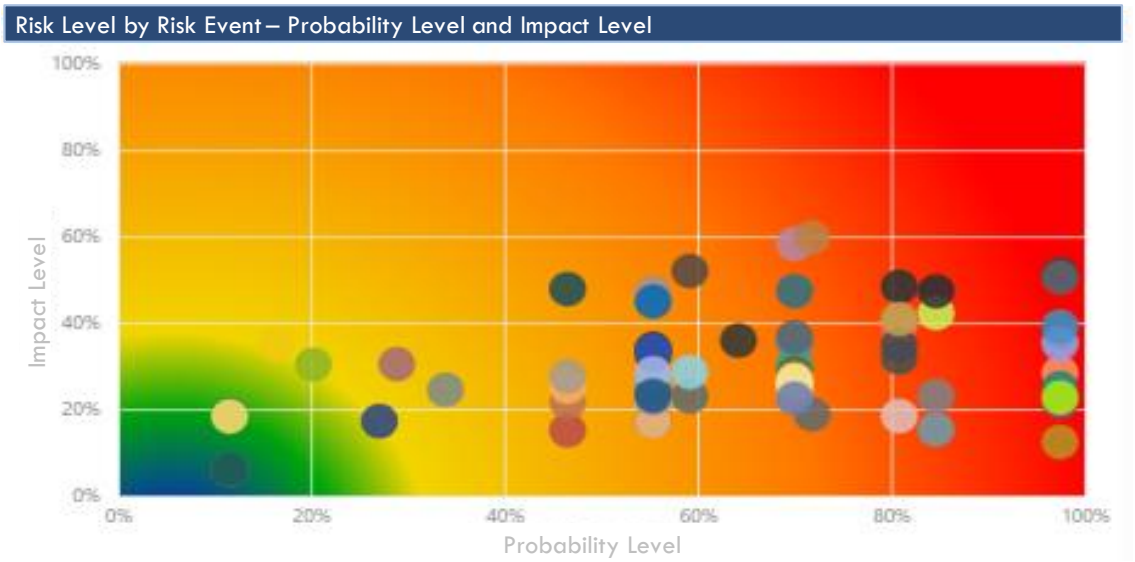
These ERM actions allowed for a reflection on the service execution, its main obstacles and the perceptions from those who are involved with the Anvisa's activities. In addition, it allowed high engagement by the multidisciplinary participation during the risk management stages and precise communication of ERM results to the different organizational levels.

In regard to the lessons learned, the implementation of the ERM Anvisa's framework at the Value Chain processes and Strategic Planning actions reinforces the need for addressing issues and risks, contributing to the organizational learning and the achievement of a greater institutional maturity degree. These initiatives enabled the Agency to enhance the implementation of ERM processes gradually and continuously, due to the complexity and comprehensiveness of the issues related to Anvisa's mission.

By prototyping the method to a pilot project, it enabled the identification of 67 risks events, which were organized according to its typology, strategic project or value chain process, organizational unit and risk lifecycle stage.

Figure 7 shows a Risk Heat Map with its risk events and related risk level using a Probability x Impact matrix.

Figure 7 - Probability x Impact Risk Heat Map



Source: Authors.

To advance the ERM strategy improvement, the Agency will implement a program to support its organizational unit needs related to risk management, by promoting the diffusion of the method and by applying the framework at all strategic units directly linked to Anvisa's Board. Soon, a comprehensive, multidimensional and intensive approach will enable the integration of the risk management process with other strategic planning actions and the value chain process, providing governance and internal control.

4. Final Considerations

This study's conclusion highlights the important method of how to apply ERM at an organization. The ERM topic is broad and complex and its implementation at an organization has been a challenge for multiple teams. The Framework and Canvas, presented in this study, are the result of the integration between theories and practices experienced by a team in their daily work over one year and a half.

As discussed above, the proposed method is a pragmatic path to be followed, since it gives a series of broken-down steps to support managers in recognizing potential risks and managing them systematically. It also facilitates decision-making and stimulates the development of an organizational ERM culture. In this sense, risk management is expected to reduce operational costs and increase social and economic benefits.

This structure is presented as an option for managers to assess public administration risks. It enables participants to be highly engaged with the possibility of concentrating efforts on the solution of a specific risk, listening to the opinions of all the participants and using the vote as an instrument to measure the risk event.

It should be noted that the Canvas is constantly evolving as an instrument and practice of governance in the public sector. Given the specificity and purpose of each organization, it can be adjusted and reconfigured to better adapt to a different context. In addition, it can be applied as often as needed, depending on the periodicity established by the organization's ERM policy. Handling risks involves making decisions that can generate losses and/or gains for the organization.

The framework can 'save time', once the main risk process stages can be experienced in short time, lasting between 4 and 8 hours. This way, it is possible to quickly assess the risks of all Value Chain processes' and to promptly identify the main risks for developing treatment plans.

Some limitations were related to the Risk Management low maturity at Anvisa, lack of risk culture at the organization, and the stakeholder´s understanding of this important governance tool. Other limitations were related to the low number of workshops to better test and develop the ERM Canvas, hence more experience would enhance the Framework and the model. Finally, there is still a need to test the Framework and ERM Canvas at different Public Administration Organizations, which will be a subject for future research.

The findings of this study contribute to the field of ERM in both knowledge production and practice of ERM. The diffusion of ERM in the Brazilian Public Administration, as in the case of Anvisa, offers opportunities for future research in this area, serving as an example to adapt the ERM methods to each organization's reality. Given the relationship between the integrated ERM approach and the appropriate use of tools and techniques that help practitioners perform their work and manage risks, the result has improved public service delivery and led to successful outcomes.

References

Abrahamson, E. (1991). Managerial fads and fashions: The diffusion and refection of innovations. Academy of Management Review, 16(3), 586–612. https://doi.org/10.5465/AMR.1991.4279484

Abrahamson, E., & Eisenman, M. (2008). Employee-management techniques: Transient fads or trending fashions? Administrative Science

Quarterly, 53(4), 719–744. https://doi.org/10.2189/asqu.53.4.719

Alves, G. de F.; Neto, W. L.; Coli, M. C.; Bermejo, P. H. de S.; Sant' Ana, T. D.; & Salgado, E. G. (2017). Perception of enterprise risk management in Brazilian higher education institutions. In: M. Themistocleous & V. Morabito (Eds.). Lecture Notes in Business Information Processing (pp. 506–512). Springer. https://doi.org/10.1007/978-3-319-65930-5_40

Brasil. (2018). Gestão de Riscos Corporativos Guia Prático de GRC. Brasília, DF: Anvisa. Retrieved from https://www.gov.br/anvisa/pt-br/acessoainformacao/acoeseprogramas/gestao-de-riscos/arquivos/1535json-file-1

Brasil. (2016). Instrução Normativa N 01/2016. Brasília, DF: Ministério do Planejamento Orçamento e Gestão, Controladoria Geral da União.

Brasil. (2017). Agência Nacional de Vigilância Sanitária - Anvisa. PORTARIA No 854, DE 30 DE MAIO DE 2017. Brasília, DF: Anvisa.

Bromiley, P.; McShane, M.; Nair, A.; & Rustambekov, E. (2015). Enterprise risk management: Review, critique, and research directions. Long Range Planning, 48(4), 265–276. https://doi.org/10.1016/j.lrp.2014.07.005

Brown, T. (2009). Change by design: How design thinking transforms organizations and inspires innovation. New York, NY: HarperCollins.

Chang, S.-I.; Huang, S.-M.; Roan, J.; Chang, I.-C.; & Liu, P.-J. (2014). Developing a risk management assessment framework for public administration in Taiwan. Risk Management, 16(3), 164–194. https://doi.org/10.1057/rm.2014.9

COSO. (2004). Enterprise risk management: Integrated framework. (Commission Committee of Sponsoring Organizations of the Treadway, Ed.). Retrieved from www.coso.org/publications.Htm

COSO. (2017). COSO enterprise risk management: Integrating with strategy and performancement. AICPA.

Damanpour, F.; Sanchez-Henriquez, F.; & Chiu, H. H. (2018). Internal and external sources and the adoption of innovations in organizations. British Journal of Management, 29(4), 712–730. https://doi.org/10.1111/1467-8551.12296

De.Vries, H.; Bekkers, V.; & Tummers, L. (2016). Innovation in the public sector: A systematic review and future research agenda. Public Administration, 94(1), 146–166. https://doi.org/10.1111/padm.12209

Denhardt, R. B. & Catlaw, T. J. (2015). Theories of public organization. Stamford: Cengage Learning.

Donnelly, R.; Clement, J.; Le Heron, R.; & George, J. S. (2012). Redesigning risk frameworks and registers to support the assessment and communication of risk in the corporate context: Lessons from a corporate risk manager in action. Risk Management, 14(3), 222–247. https://doi.org/10.1057/rm.2012.3

Eppler, M. J. & Aeschimann, M. (2009). A systematic framework for risk visualization in risk management and communication. Risk Management, 11(2), 67–89. https://doi.org/10.1057/rm.2009.4

Hansson, S. O. (2001). Framework for public management. Risk Management, 3(3), 23–32.

Hillson, D. (2016). The risk management handbook: A practical guide to managing the multiple dimensions of risk. (D. Hillson, Ed.). KoganPage. London: KoganPage. Retrieved from http://www.theirm.org/publications/PUstandard.html

ISO. (2009). ISO 31000. Risk management - Principles and guidelines. International Organizational for Standardization.

ISO. (2018). ISO 31000 Risk management - Risk assessment techniques. International Organizational for Standardization. Retrieved from https://www.iso.org/about-us.html

Martins, M. A. F.; Santos, W. O. dos; Brito, R. L. de; & Alves, G. de F. (2017). Política de gestão de riscos corporativos: O caso de uma agência reguladora da saúde. Revista Do Serviço Público, 69(1), 7–32. Retrieved from https://repositorio.enap.gov.br/handle/1/3260

Moore, M. H. (2013). Recognizing public value. Harvard University Press.

OGC. (2010). Management of risk : Guidance for practitioners. Axelos. London: Office of Government Commerce - Axelos.

Osterwalder, A. & Pigneur, Y. (2010). Business model generation: A handbook for visionaries,

game changers, and challengers. New Jersey: John Wiley & Sons.

Paulo Henrique de Souza Bermejo; Sant'Ana, T. D.; Salgado, E. G.; Mendonça, L. C.; Anjos, F. H. dos; Alves, G. de F.;& Neves, T. J. G. das. (2019). ForRisco: gerenciamento de riscos em instituições públicas na prática (2nd ed.). Evobiz.

Pollitt, C., & Bouckaert, G. (2011). Public management reform: A comparative analysis. Oxford University Press. USA: Oxford.

Power, M. (2004). The risk management of everything. The Journal of Risk Finance, 5(3), 58–65. https://doi.org/10.1108/eb023001

Power, M. (2009). The risk management of nothing. Accounting, Organizations and Society, 34(6–7), 849–855. https://doi.org/10.1016/j.aos.2009.06.001

Santos, C. D. dos; Silva, J. A. da; Silva, D. A. da; & Alves, G. de F. (2018). Gestão de riscos no setor público: Revisão bibliométrica e proposta de agenda de pesquisa. In: 15th International Conference On Information Systems & Technology Management - CONTECSI - 2018 (pp. 774–794). São Paulo. https://doi.org/10.5748/9788599693148-15CONTECSI/DOCT-5561

Stein, V. & Wiedemann, A. (2016). Risk governance: Conceptualization, tasks, and research agenda. *Journal of Business Economics*, *86*(8), 813–836. https://doi.org/10.1007/s11573-016-0826-4

Gustavo de Freitas Alves

https://orcid.org/0000-0001-5142-5250

PhD in Administration at University of Brasília - UnB (2020). Master´s in applied computer science at UnB (2015). Consultant for over 15 years with broad experience in Information Technology, ability to translate business needs into action, advising teams and organizations. Practical and academic abilities to deal with complex problem.

E-mail: gustavo@hepta.com.br

Mary Anne Fontenele Martins

https://orcid.org/0000-0002-8391-7695

Specialization and Master's degree in Public Health from the Federal University of Ceará (2003). PhD student in Public Health at the University of Brasília. Knowledge in health surveillance, management, strategic health planning & assessment, and application of risk identification and management techniques in public organizations.

E-mail: mary.martins@anvisa.gov.br

Rodrigo Lino de Brito

https://orcid.org/0000-0002-4647-6958

Master's degree (2007) in Public Health at Fundação Oswaldo Cruz (Fiocruz). Has experience in Public Management and Public Health fields. Since 2011, has worked as a Specialist in Public Policy and Government Management, developing projects in the areas of Planning, Governance and Innovation at the Ministry of Economy.

E-mail: rodrigo.l.brito@economia.gov.br

Wildenildo Oliveira dos Santos

https://orcid.org/0000-0003-4590-249X

Specialist in Public Administration by the University of Piauí (2005), in Health Surveillance by FIOCRUZ (2011) and in Health Surveillance Management by Instituto Sírio Libanês (2012), public servant at Anvisa (2007), experience in strategic planning, project management , regulatory quality, business processes and corporate risk management.

E-mail: wildenildo.santos@anvisa.go