# An Applied Risk Identification Approach in the ICT Governance and Management Macroprocesses of a Brazilian Federal Government Agency

Edna Dias Canedo[1][a], Ana Paula Morais do Vale[2], Rogério Machado Gravina[2],
Rafael Leite Patrão[2][b], Leomar Camargo de Souza[1][c], Vinicius Eloy dos Reis[3],
Fábio Lúcio Lopes Mendonça[2][d] and Rafael T. de Sousa Jr.[2][e]

[1]*Department of Computer Science, University of Brasília (UnB), Brasília, DF, Brazil*

[2]*National Science and Technology Institute on Cyber Security, Electrical Engineering Department, University of Brasília (UnB), Brasília, DF, Brazil*

[3]*General Coordination of Information Technology (CGTI), Administrative Council for Economic Defense (CADE), Brasília, DF, Brazil*

Keywords: Macroprocesses of ICT Management and Governance, Risk Identification, Provide ICT Governance, Provide ICT Infrastructure, Tools and Techniques.

Abstract: Risk management is of great importance, both in the risk management of private organizations and in public administration organizations. Thus, in order to guarantee effective risk management and properly aligned with the organizational objectives, it is necessary to map and continuously evaluate the possible risks that may impact the organization's service provision. This work presents the identification of the risks of the Macroprocesses of Management and Governance of Information and Communication Technology (ICT) of a federal public administration agency. The identification and classification of risks were carried out using the integrity and risk management support system (AGIR). The classification of ICT risks carried out will support stakeholders in decision making, allowing for a better assessment and quality of ICT services provided by the organization to its users.

## 1 INTRODUCTION

The process of providing Information and Communication Technology (ICT) governance contains several uncertainties. One way to address the uncertainties involved in this process is to understand how the risks are inserted in the internal and external context of the organization. Risks are the effects of uncertainty on organizational goals, leading to a deviation from what is expected, which can be positive (an opportunity) or negative (Barafort et al., 2019). The ICT governance risk assessment process, together with specific tools and techniques, assists managers in decision making, allowing them to understand the exposure and the potential impact of risks tool organizational objectives. It is the responsibility of the ICT manager to align her/his actions to the organization's strategic plan and to seek techniques and tools to support it. This is done so that decision-making guarantees the best evaluation, the best performance, or the best agreement between the stakeholders' expectations.

Joint Normative Instruction (INC) No. 1, of May 10, 2016, provides for the internal controls, risk management, and governance of ICT, which defines that the agencies and entities of the Brazilian federal executive power must implement, maintain, monitor, and review the risk management process, compatible with its mission and its strategic objectives, observing the guidelines established in the INC. In addition, it is defined that the bodies can use ISO/IEC 31000 (ISO/IEC, 2018b) and COSO (Moeller, 2007) as risk management references.

The ISO/IEC 31000 guidelines and implementation guide are applicable to all types and sizes of organizations, as they all face external and internal influences and factors that may interfere with the achieve-

[a] https://orcid.org/0000-0002-2159-339X
[b] https://orcid.org/0000-0003-1546-2972
[c] https://orcid.org/0000-0003-1230-9235
[d] https://orcid.org/0000-0001-7100-7304
[e] https://orcid.org/0000-0003-1101-3029

Canedo, E., Morais do Vale, A., Gravina, R., Patrão, R., Camargo de Souza, L., Reis, V., Mendonça, F. and Sousa Jr., R.
An Applied Risk Identification Approach in the ICT Governance and Management Macroprocesses of a Brazilian Federal Government Agency.
DOI: 10.5220/0010475902720279
In *Proceedings of the 23rd International Conference on Enterprise Information Systems (ICEIS 2021) - Volume 1*, pages 272-279
ISBN: 978-989-758-509-8

ment of their objectives. According to ISO/IEC 31000 (ISO/IEC, 2018b), risk management must be based on outlined principles, structure, and processes. Regarding the structure of risk management, the standard defines that its purpose is to support the organization in the integration of risk management in significant activities and functions, this requires the support of interested parties, mainly from senior management. The development of the risk structure includes integration, design, implementation, evaluation, and improvement of risk management through the organization (ISO/IEC, 2018b).

In view of the scenario of the federal public administration agencies, we present in this article the risk identification of the Macroprocess entitled: Management and Governance of ICT. This is a competency of CADE's General Coordination of Information Technology (CGTI) and the tool used for the assessment was the Support System Integrity and Risk Management (AGIR). The risk mapping will allow the organization's risk management officer to find ways to minimize the risks in ICT management and governance, offering a decision model to support the manager in the provision of ICT services, in his constant and routine assessment and decision making on existing alternatives for the provision of ICT services.

## 2 RISK MANAGEMENT

Managing risks is an interactive activity and assists organizations in establishing strategies to achieve their goals and decision-making (ISO/IEC, 2018b). In addition, managing risks contributes to the improvement of organizational management systems (Hanggraeni et al., 2019). Managing risks is part of all activities associated with an organization and includes interaction with stakeholders. Managing risks considers the external and internal contexts of the organization, including human behavior and cultural factors (ISO/IEC, 2018b).

The purpose of risk management is to create and protect value, improving performance, encouraging innovation, and supporting the achievement of organizational objectives. Principles are the basis for managing risks and need to be considered when establishing the organization's risk management structure and processes (Otto, 2020). The effectiveness of risk management depends on its integration with ICT governance and with all other organization's activities, including decision making (de Araújo Lima et al., 2020). Risk management requires the support of stakeholders, in particular, senior management (Bernard, 2012). It is important that senior management and supervisory bodies (where applicable) ensure that risk management is integrated with all activities of the organization (Ghani and Farisya, 2019). Senior management is responsible for managing risks, while supervisory bodies are responsible for supervising risk management (ISO/IEC, 2018b).

In ICT management, concern about risks is a key aspect, as it ensures that strategic business objectives are not put at risk by ICT failures. The risks associated with technical problems are increasingly evident on the managers' agendas, given that the impact on the business of this type of failure can have serious consequences, especially in the case of organizations with high strategic dependence on ICT (Netto and Fernandes, 2013). In this sense, the investigation of the elements of risk analysis, with regard to the economic issues of the organization, has become an area of importance, as there are rare situations where economic decisions are made in ideal scenarios (Rana et al., 2019). The sources of uncertainty are diverse and extensive, and include risks related to the most diverse concepts (Bejinariu, 2020). Because of this, decisions made under risky situations, both public and private, are of considerable interest (Chavas, 2004).

The information security risk regulation (ISO/IEC, 2018a) provides pertinent information on how the interactivity of risk management activities takes place. According to the document, it is necessary initially to establish the context and then carry out the risk assessment process. The result of this process is then subjected to an assessment with the purpose of verifying whether the information generated is sufficient to determine the necessary actions to reduce the risk to an acceptable level. If sufficient this step is completed and the risk treatment process can be followed, if not, a new iteration is performed, again evaluating the context, and criteria used, possibly in limited parts of the scope (ISO/IEC, 2018a).

It is important to note that the effectiveness of the risk treatment process depends on the results obtained in the assessment stage. To carry out this process, it is necessary to apply in a cyclical manner the activities of (i) evaluating a risks treatment, (ii) deciding whether the residual risk levels are acceptable, (iii) generating a new treatment of the risk if the levels of risks are not acceptable and (iv) evaluate the effectiveness of the treatment (ISO/IEC, 2018a). At the end of the treatment, there is a possibility that the residual risk level obtained is not satisfactory in this case another iteration of the risk assessment process may be necessary, with the aforementioned recommendations, but with the addition of an additional treatment step of risks (ISO/IEC, 2018a).

For a risk to be accepted, residual risks must be explicitly accepted by stakeholders, especially when there are important decisions about whether or not to implement controls. Therefore, for there to be accepted, it is important to communicate correctly about the whole process, from identification and treatment, so that interested parties can manage possible incidents and also provide assistance in activities involving these steps (ISO/IEC, 2018a).

In the private sector, large audit institutions already use the concept of risk in their audit models or work processes, alongside sampling and the evaluation of internal controls, as tools to minimize economic restrictions on audit activity (Freitas, 2002). Most risk considerations are common among public and private organizations, however, some differences between risk approaches in the public and private sectors are that, while in public companies the focus is on agencies and programs, the private sector prioritizes the business. . This is due to the public sector having systemic risk, where there is dependence on various organizations. Another consideration is that, while the public sector aims at the continuity of services, private companies focus on profit, that is, value for the customer instead of public value (value for the citizen) (Hood and Rothstein, 2000).

# 3 STUDY SETTINGS

The main goal of this article is to present the stages of risk identification of the ICT management and governance Macroprocesses of the General Coordination of Information and Communication Technology (CGTI). We will present in detail the risks identified for the processes: a) Provide ICT Governance; and b) Provide ICT infrastructure. For the risk identification stage, there are several techniques and tools that can be applied to assist those responsible for this activity, and each has its particularities. At different times in the cyclical risk management process, different tools may be needed. In addition, understanding which is the best technique is an important step of the context setting stage. Each organization must analyze which of the existing tools is best suited to their organizational needs.

The ISO/IEC 31000 (ISO/IEC, 2019) standard, referring to techniques for the risk assessment process, presents some recommendations of tools and techniques, both for the risk identification step and for the subsequent steps, such as risk assessment and analysis. Borges (Borges, 2018) classified the main techniques and tools of the ISO/IEC 31000 standard, according to their applicability in each stage of the risk assessment process. According to this classification, and in the recommendations presented in ISO/IEC 31000 (ISO/IEC, 2019), we select the techniques that are suitable for the risk identification stage, as shown in Table 1.

Table 1: Tools and Techniques (Borges, 2018; ISO/IEC, 2018b; ISO/IEC, 2019).

| Tools and Techniques | Risk Identification |
|---|---|
| Brainstorming | Strongly Suitable |
| Verification List | Strongly Suitable |
| Structured or semi-structured interviews | Strongly Suitable |
| Human reliability analysis | Strongly Suitable |
| Delphi | Strongly Suitable |
| HAZOP | Strongly Suitable |

Ferreira (Ferreira, 2017) presented a consolidation of the techniques and tools most used in the risk assessment process. The author proposed a risk management model/process that used the technique of agile methodologies to assess the identified risks. Table 2 presents the techniques consolidated by the author, with the most suitable techniques and tools in the risk identification stage and their use frequency. In this research, we used the techniques presented in Table 2 to carry out the risk assessment. It is possible to check through the information presented in Tables 1 and 2 the recurrence of some techniques. This is an important fact that can contribute to the initial choice of methodology to carry out risk identification in an organization. Thus, this recurrence impacted our choice of the techniques and tools selected to carry out the identification and validation of risks in our case study.

Table 2: Use frequency of techniques and tools for risk assessment (Ferreira, 2017).

| Tools and Techniques | Use frequency |
|---|---|
| Semi-structured interviews | 5 |
| Brainstorming | 4 |
| Literature review based on scientific articles | 4 |
| Historical database of typical risks (owned or shared) | 3 |
| Questionnaire | 3 |

## 3.1 Organization Overview

The General Coordination of Information and Communication Technology (CGTI) is one of the coordinations that make up CADE's Administration and

Planning Directorate (DAP). The Information Technology Master Plan (PDTI) 2017-2020 is the strategic reference of the coordination, which comprises the mission, vision and values of the ICT unit. CGTI's strategic objectives are established in the PDTI, with a view to contributing to the organization's objectives. Figure 1 shows CGTI's strategic planning ICT.

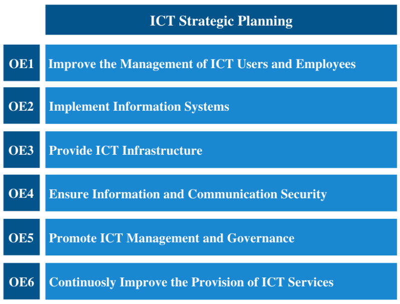
ICT Strategic Planning
OE1
Improve the Management of ICT Users and Employees
OE2
Implement Information Systems
OE3
Provide ICT Infrastructure
OE4
Ensure Information and Communication Security
OE5
Promote ICT Management and Governance
OE6
Continuosly Improve the Provision of ICT Services

Figure 1: ICT Strategic Planning.

CADE has an ICT governance structure so that each organizational unit and its risk managers periodically identify, prioritize, monitor, and report to the Integrity, Risk Management, Governance and Internal Controls Committee (CORISC), the main risks and mitigation actions that were planned. In addition, the president of CADE and the general superintendent are primarily responsible for establishing the organization's strategy and risk management structure. The risk management process can be applied to the strategic, operational, program, or project levels in the organization.

# 4 RESULTS AND DISCUSSION

## 4.1 Provide ICT Governance

According to ISO/IEC 38500 (ISO/IEC, 2018c), ICT governance is the system by which the current and future use of ICT is directed and controlled in the organization. Within the scope of CADE, the Management Services and Governance (SEGOV) has as one of its attributions to manage the risks related to ICT management and governance, its other attributions are presented in Table 3.

Table 3: SEGOV responsibilities.

| SEGOV Responsibilities |
|---|
| Plan, coordinate and guide the procurement and contract management actions related to management and governance. |
| Manage projects related to ICT management and governance. |
| Deploy and sustain management and governance solutions. |
| Identify, evaluate and propose technology solutions to support CADE's final activities. |
| Propose policies and guidelines regarding the planning, implementation and maintenance of activities related to ICT governance. |
| Formulate and maintain ICT governance and management model. |

In its PDTI, CGTI also listed its ICT needs regarding the strategic objective of Promoting ICT Management and Governance, which were considered at the stage of establishing the context for identifying risks, which are: 1)Implement and formalize the ICT Risk Management processes, ICT Business Continuity, Contracting and Management of ICT Goods and Services Contracts, ICT Governance, Portfolio Management and ICT Projects and ICT Service Management; 2)Knowledge management project; 3)Standardization of Contracting Artifacts and Acquisition of ICT assets and; 4)Implementation of the data quality and integration solution. In a case study carried out within the scope of CADE by Canedo et al. (Canedo et al., 2020), after applying a questionnaire to CGTI members/employees, the authors identified among the processes not defined and not implemented, the ICT Service Continuity processes, ICT project management and ICT Service Management. In addition, the authors identified the absence of some artifacts related to the ICT processes that were already implemented at CADE.

Thus, based on the strategic objectives of the PDTI, the needs of ICT and the assignments of SEGOV, we started the identification of risks in the process of Providing Management and Governance of ICT. In this initial phase, we use the Brainstorming technique with the CGTI team, the Table 5 presents the identified risks, their causes and possible effects, the typology of the risk event, as well as pointing out internal controls that already exist CGTI referring to each identified risk. Once the risk events related to the ICT management and governance process were identified by the CGTI team, the risk assessment process defined by the ISO 31000 (ISO/IEC, 2018b) standard can proceed to the next step, risk analysis, which aims to understand the nature and characteristics of the risks identified.

## 4.2 Provide ICT Infrastructure

In CADE's context, ICT management and governance is a macro-process that has several linked level 1 processes. Among them is the process of Provide ICT

Infrastructure. The CGTI has subordinate sectors responsible for exercising attributions that help the development of its macro-process, and the unit responsible for the process Provide ICT Infrastructure is the Security and Infrastructure Service (SESIN) The application of the Risk Management process according to ISO/IEC 31000 (ISO/IEC, 2018b) has several stages, and it is important that the activities inherent to each phase of the process are respected.

The context-setting phase reinforces the need for specific techniques and tools, as well as the approach and important documentation definition to help identify risks. Among the identified inputs, we have the PDTI, from which information was extracted. This information was related to CADE's ICT needs involving the ICT strategic objective related to Providing ICT Infrastructure and ICT Management and Governance. In addition, we also analyzed the ICT Strategic Plan (PETIC), as there is a capillarity of the information provided in both documents, PDTI and PETIC, since the strategic objectives of ICT are defined in PETIC.

In addition to these documents, the factors considered important to be included in the ICT risk identification stage were extracted from the ISO/IEC 310000 (ISO/IEC, 2018b), these factors can be seen in Table 4. The identification of risks took into account the duties of SESIN to define the risks inherent in the process Provide ICT Infrastructure, and through the application of the defined techniques and tools (Tables 1 and 2) and based on the factors listed in the standard, the risks described in Table 6 were identified within CADE's infrastructure team. It is important to highlight that, for the risks of the process of Provide ICT Infrastructure, only the first identification stage was carried out, where it is necessary to submit the items to critical analysis so that the risks are validated by the managers. The risks identified in the Provide ICT Infrastructure sub-process will be monitored and validated with the teams involved in SESIN's assignment activities and, if necessary, possible adjustments will be made. In the future, we will propose a contingency plan to mitigate the identified risks.

Table 4: Factors to be considered when identifying risks.

| **Risk Identification: Factors** |
|---|
| Tangible and intangible sources of risk |
| Causes and events |
| Threats and opportunities |
| Vulnerabilities and capabilities |
| Changes in external and internal contexts |
| Emerging risk indicators |
| Nature and value of assets and resources |
| Consequences and their impacts on objectives |
| Limitations of knowledge and reliability of information |
| Time factors |
| Biases, hypotheses and beliefs of those involved |

## 5 THREATS TO VALIDITY

The present work has some threats that can limit or even compromise our results. The first is related to the difficulty of communication with the members of CADE's ICT governance team, as this factor may have contributed to different factors, such as: (i) survey of irrelevant or superficial risks to the context of the organization; (ii) potential risks ignored due to little knowledge of the areas involved; and (iii) the complete non-validation of all risks identified during the risk identification process. To try to mitigate these risks, we held several meetings with the organization's ICT governance participants to present and discuss the risks identified. It is also important to highlight a possible external risk that is related to the cadre of people that make up CADE's ICT team, where currently, the majority of the team is made up of non-effective employees and with that, some risks may not have been identified in our research, due to the lack of knowledge of some employees in relation to the organization's ICT Management and Governance processes. However, in order to mitigate this risk, we held meetings with managers to validate the risks identified and discuss the perception of employees. Finally, the last threat is related to the fact that ICT processes are not fully mapped by the ICT management and governance team. This can give members of the ICT governance team a limited view of the possible risks related to their activities and their impacts on the organization.

## 6 CONCLUSION

This work allowed those involved to understand the initial steps regarding the risk management process. The study of the regulations was important to know the activities corresponding to the definition of the context and identification of the risks of ICT. It was possible to verify that with the development of the steps for defining techniques and tools for the identification of risks, it was possible to obtain important inferences and insights with the stakeholders in the definition of the factors to be considered to identify the risks relevant to the context of the organization.

Table 5: Risk Events Identified in the ICT Management and Governance Process.

| **Events** | **Causes** | **Effects** | **Typology** | **Internal Control** |
|---|---|---|---|---|
| R01. Failures in the implementation of the Risk Management process at CGTI | 1. Lack of knowledge and awareness about risk management for all team members<br>2. Failure to prioritize the risk management process<br>3. Failure to implement the AGIR system | 1.Exposure to risks that may affect the business<br>2. Non-compliance with best practices and regulations (compliance)<br>3. Accountability | Operational | 1. Ordinances and rules regarding risk management at CADE |
| R02. Non-formalization of project management methodology | 1. Team members with experience in projects cause non-prioritization of the process<br>2. Some members lack basic knowledge on projects<br>3. Low standardization of project management concepts | 1. Delay in project delivery<br>2. Failure to achieve the expected results<br>3. Non-standard in project management | Operational | |
| R03. Failures in the management of ICT human resources | 1. Lack of corporate people management systems<br>2. Failure in setting new employees<br>3. Lack of performance measurement procedures<br>4. Development of leaders on topics related to people management | 1. High turnover of servers<br>2. Difficulties in the continuity of processes<br>3. Low performance of employees | Operational | 1. Norms related to people management |
| R04. Non-implementation of knowledge management | 1. Low culture of knowledge management<br>2. Lack of process definition | 1. Loss of organizational<br>2. Discontinuity | Operational Knowledge | |
| R05. Failure to deliver CGTI value to the business | 3. Failure to prioritize knowledge management<br>1. Failure in the strategic alignment between business and ICT<br>2. Failure in how the ICT area communicates its relevance to senior management<br>3. Failures in the governance structures of CADE | 3. Rework in training new employees<br>1. Failing to deliver expected results and actions<br>2. Failure in budget execution<br>3. Impact on achieving the objectives of the organization<br>4. Understanding effort and resources in non-relevant initiatives | Strategic | 1. Governance standards |

Table 6: Risk Events identified in the Provide ICT Infrastructure process.

| **SESIN** | |
|---|---|
| **Work Process** | **Risk** |
| Plan, coordinate and guide the acquisition and management of infrastructure contracts | 1. Lack of technical knowledge of the product or equipment to be purchased<br>2. Lack of knowledge of laws and regulations<br>3. Failure to communicate project requirements and needs<br>4. Poorly dimensioned service provision contracts related to ICT activities<br>5. Lack of budgetary resources for acquisitions |
| Manage infrastructure-related projects | 1. Poorly designed project scope<br>2. Poorly sized team for managing demands |
| Deploy and sustain communication and connectivity solutions | 1. Lack of training for the responsible team<br>2. Difficulty in accessing the organization's systems and resources<br>3. Failure of network assets<br>4. Internet link unavailability<br>5. Failure to back up data before deploying a solution |
| Manage infrastructure-related risks | 1. Unavailability of systems<br>2. Longer incident response time<br>3. Failure in the institution's logical or physical network |
| Identify, evaluate and propose technology solutions to support CADE's final activities | 1. Hiring obsolete technology solutions<br>2. Lack of access to systems and resources due to lack of licensing<br>3. Poor assessment of the needs of the final areas by the ICT area<br>4. Data exposure due to acquired solution vulnerability |
| Coordinate the support of ICT assets | 1. Lack of maintenance contracts<br>2. Lack of trained personnel to support ICT assets<br>3. Lack of help desk contracts |
| Assist users in the operation of ICT assets | 1. Lack of knowledge of the help desk in relation to some organization's systems<br>2. Lack of communication regarding the operation of ICT assets |
| Maintain operability of the CADE secure room | 1. Interruption of electricity supply<br>2. Air conditioning equipment failure<br>3. Failure in the standby generator in the event of a power interruption<br>4. Lack or failure of preventive maintenance<br>5. Unauthorized physical access<br>6. Difficulty in physical access to the secure room |

This allows for standardization and decentralization of activities inherent to the process, allowing modeling to be carried out in such a way that the organization is able to define a standard, according to its needs. In our findings, it is possible to conclude that, due to the cyclic nature of the risk management process it is possible to apply different techniques in the same steps, but in different situations, that is, it is not necessary to define a specific technique for each step of the process, but to define a set of techniques and tools at different times for the same stage. As future work, we will carry out the identification of the risks of the other processes at level 1, and analyze whether the techniques and tools used will also adhere to the other processes. In addition, we will apply the risk identification process to other organizations and carry out a comparison of the results, ranking the techniques and tools most adherent to each process.

## ACKNOWLEDGMENTS

The authors would like to thank the support of the Brazilian research, development and innovation agencies CAPES (grants 23038.007604/2014-69 FORTE and 88887.144009/2017-00 PROBRAL), CNPq (grants 312180/2019-5 PQ-2, BRICS2017-591 LargEWiN, and 465741/2014-2 INCT in Cybersecurity) and FAP-DF (grants 0193.001366/2016 UIoT and 0193.001365/2016 SSDDC), as well as the cooperation projects with the Ministry of the Economy (grants DIPLA 005/2016 and ENAP 083/2016), the Institutional Security Office of the Presidency of the Republic (grant ABIN 002/2017), the Administrative Council for Economic Defense (grant CADE 08700.000047/2019-14), and the General Attorney of the Union (grant AGU 697.935/2019).

## REFERENCES

Barafort, B., Mesquida, A. L., and Mas, A. (2019). ISO 31000-based integrated risk management process assessment model for IT organizations. *J. Softw. Evol. Process.*, 31(1).

Bejinariu, R. M. (2020). Study concerning risk assessment related to organizational business processes. In *Sustainable Business Performance and Risk Management*, pages 67–92. Springer.

Bernard, P. (2012). *COBIT® 5-A management guide*. Van Haren.

Borges, N. F. (2018). Proposta de ferramenta de risco aplicável em projetos que utilizam o scrum. *Faculdade de Tecnologia, Engenharia de Produção, Universidade de Brasília (UnB)*, page 70.

Canedo, E. D., do Vale, A. P. M., Patrão, R. L., de Souza, L. C., Gravina, R. M., dos Reis, V. E., de Mendonça, F. L. L., and de Sousa Jr., R. T. (2020). Information and communication technology (ICT) governance processes: A case study. *Inf.*, 11(10):462.

Chavas, J.-P. (2004). Risk analysis in theory and practice. *Risk Analysis in Theory and Practice*.

de Araújo Lima, P. F., Crema, M., and Verbano, C. (2020). Risk management in smes: A systematic literature review and future directions. *European Management Journal*, 38(1):78–94.

Ferreira, E. C. (2017). Proposta de metodologia de gestão de riscos para projetos ágeis de software no instituto nacional de estudos e pesquisas anísio teixeira (inep). *Universidade de Brasília (UnB), Brasil*, page 149.

Freitas, C. A. S. d. (2002). Gestão de risco: Possibilidades de utilização pelo setor publico e por entidades de fiscalização superior. *Revista do TCU*, page 13.

Ghani, E. K. and Farisya, S. (2019). Effect of employees' competency, risk culture and organizational innovativeness on enterprise risk management implementation. *International Journal of Innovation, Creativity and Change*, 8(3):173–186.

Hanggraeni, D., Ślusarczyk, B., Sulung, L. A. K., and Subroto, A. (2019). The impact of internal, external and enterprise risk management on the performance of micro, small and medium enterprises. *Sustainability*, 11(7):2172.

Hood, C. and Rothstein, H. (2000). Business risk management in government: Pitfalls and possibilities. *SSRN Electronic Journal*.

ISO/IEC (2018a). *ISO/IEC 27005:2018: Information technology — Security techniques — Information security risk management.* Number ISO/IEC 27005:2018. ISO—-International Organization for Standardization, 3 edition.

ISO/IEC (2018b). *ISO/IEC 31000:2018: Risk management — Guidelines.* Number ISO/IEC 31000:2018. ISO—-International Organization for Standardization, 2 edition.

ISO/IEC (2018c). *ISO/IEC 38500:2018: Information Technology — Governance of IT for the organization.*, volume ISO/IEC 38500:2018. ISO—-International Organization for Standardization, 2 edition.

ISO/IEC (2019). *ISO/IEC 31010:2019: Risk management — Risk assessment techniques.* Number ISO/IEC 31010:2019. ISO—-International Organization for Standardization, 2 edition.

Moeller, R. R. (2007). *COSO enterprise risk management: understanding the new integrated ERM framework*. John Wiley & Sons.

Netto, S. and Fernandes, A. (2013). Proposta de artefato de identificação de riscos nas contratações de TI da administração pública federal, sob a ótica da ABNT NBR ISO 31000 : gestão de riscos.

Otto, L. (2020). It-governance in integrated care: A risk-centred examination in germany. In *HEALTHINF*, pages 808–817. SCITEPRESS.

Rana, T., Wickramasinghe, D., and Bracci, E. (2019). New development: Integrating risk management in management control systems—lessons for public sector managers. *Public Money & Management*, 39(2):148–151.