OECD Public Governance Reviews

Modernising Integrity Risk Assessments in Brazil

TOWARDS A BEHAVIOURAL-SENSITIVE AND DATA-DRIVEN APPROACH

OECD

OECD Public Governance Reviews

Modernising Integrity Risk Assessments in Brazil

TOWARDS A BEHAVIOURAL-SENSITIVE AND DATA-DRIVEN APPROACH

OECD
BETTER POLICIES FOR BETTER LIVES

Please cite this publication as:
OECD (2022), *Modernising Integrity Risk Assessments in Brazil: Towards a Behavioural-sensitive and Data-driven Approach*, OECD Public Governance Reviews, OECD Publishing, Paris, https://doi.org/10.1787/ad3804f0-en.

ISBN 978-92-64-57600-1 (pdf)
ISBN 978-92-64-51337-2 (HTML)
ISBN 978-92-64-85843-5 (epub)

OECD Public Governance Reviews
ISSN 2219-0406 (print)
ISSN 2219-0414 (online)

Photo credits: Cover © Marcello Casal Jr - Agência Brasil, Brasília-DF.

Corrigenda to publications may be found on line at: www.oecd.org/about/publishing/corrigenda.htm.

Foreword

To ensure that integrity policies are relevant, efficient and effective, integrity risks have to be adequately identified, assessed and mitigated. According to the *OECD Recommendation on Public Integrity*, risks to public integrity include not only corruption and fraud but also practices that, while unethical, may not be illegal. Despite the importance of integrity risk management, many countries face significant challenges in implementing an integrity risk management culture in their public administrations. Indeed, the value of risk management is not always clear to public managers.

Understanding why integrity risk management matters requires a clear understanding of the values and objectives of the public function in question. Such an understanding can be difficult to achieve if clear objectives, a performance culture, or robust accountability are lacking, especially given the difficulty of quantifying public sector impact and productivity. In addition, public managers may lack the necessary capacity, knowledge and support to manage integrity risks effectively.

Many of these challenges apply to Brazil, which, through the Office of the Comptroller General of the Union, is seeking to strengthen its policies, methods and institutions for promoting integrity in the federal executive branch. This report is part of a project through which the OECD supports these efforts by the Office, which leads integrity policies at the federal level. The project has three components: a review of the integrity risk assessment methodology; the application of behavioural insights to public integrity; and strengthening the Integrity Management Units (UGI) within the Public Integrity System of the Federal Executive Branch (SIPEF).

This report contributes to OECD work to support countries in effectively implementing the *OECD Recommendation on Public Integrity*. It provides an analysis and concrete recommendations on improving the implementation of integrity risk management in the Brazilian federal executive. In addition, this report provides an input to the forthcoming *OECD Integrity Review of Brazil*.

The review was approved by the OECD Working Party of Senior Public Integrity Officials (SPIO) on 13 April 2022 and declassified by the Public Governance Committee on 5 May 2022.

Acknowledgements

The report was prepared by the OECD Public Sector Integrity Division of the Directorate for Public Governance under the leadership of Elsa Pilichowski, OECD Director for Public Governance and Julio Bacio Terracino, Head of the Public Sector Integrity Division. The report was co-ordinated and drafted by Frédéric Boehm and Camila Gomes Gomes. Gavin Ugale provided invaluable guidance, support and input to the analysis and the recommendations. Estela Souto provided support with preliminary background research and the design of the questionnaire. Editorial and administrative assistance was provided by Meral Gedik.

The OECD thanks the Minister of the Office of the Comptroller General of the Union (*Controladoria-Geral da União*, CGU), Wagner de Campos Rosário, as well as his staff, in particular the Secretariat of Transparency and Corruption Prevention (*Secretaria de Transparência e Prevenção da Corrupção*, STPC), Roberto Cesar de Oliveira Viegas and Claudia Taya, as well as the Directorate for Integrity Promotion (*Diretoria de Promoção da Integridade*, DPI), Pedro Ruske Freitas, Carolina Souto Carballido and Allison Roberto Mazzuchelli Rodrigues for their support in organising the virtual fact-finding and for the many fruitful discussions on preliminary findings and recommendations throughout the project.

The OECD would also like to thank the individuals and organisations who took part in the process and provided valuable information for the preparation of the report. In particular, the OECD is grateful for the feedback and information shared by the Technical secretariat of the Public Ethics Commission (*Comissão de Ética Pública*, CEP), the Federal Ombudsman Office of the Union (*Ouvidoria-Geral da União*), CGU's Federal Secretariat of Internal Control (*Secretaria Federal de Controle Interno*) and the Integrity Management Units of the following federal entities that participated in the Focus Group and bilateral interviews: National Agency for Telecommunications (*Agência Nacional de Telecomunicações*), National Department of Transport Infrastructure (*Departamento Nacional de Infraestrutura de Transportes*), Ministry of Citizenship (*Ministério da Cidadania*), Ministry of Women, Family and Human Rights (*Ministério da Mulher, da Família e dos Direitos Humanos*), Ministry of Agriculture, Livestock and Supply (*Ministério da Agricultura, Pecuária e Abastecimento*), Ministry of Education (*Ministério da Educação*), Federal University of Maranhão Foundation (*Fundação Universidade Federal do Maranhão*), Federal Institute of Education, Science and Technology of Santa Catarina (*Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina*), National Film Agency (*Agência Nacional do Cinema*), Brazilian Institute for the Environment and Renewable Natural Resources (*Instituto Brasileiro do Meio Ambiente e dos Recursos Naturais Renováveis*), Ministry of Infrastructure (*Ministério da Infraestrutura*), Ministry of Tourism (*Ministério do Turismo*), General Secretariat of the Presidency of the Republic (*Secretaria-Geral da Presidência da República*), National Health Foundation (*Fundação Nacional de Saúde*), Superintendence for the Development of the Midwest (*Superintendência de Desenvolvimento do Centro-Oeste*), Ministry of Economy (*Ministério da Economia*) and Office of the Comptroller General of the Union (*Controladoria-Geral da União*). Finally, the OECD thanks the 30 Integrity Management Units that provided answers to the questionnaire sent out in 2020.

Table of contents

FIGURES

TABLES

Executive summary

Risk management is at the heart of any strategy or approach to ensure and promote public integrity. Although in the public sector the normative and policy frameworks for risk management are usually aligned with international standards, the actual implementation of risk management frameworks into day-to-day practice often lags behind. Challenges around managing integrity risks may be even stronger and more complex, given that corruption and fraud are sensitive and complex topics.

In Brazil's federal executive, integrity risk management became mandatory for all public entities in 2017. Integrity risk management is a key element of the Integrity Programmes and the Integrity Plans that have been established since 2017 in all 186 entities of the federal executive. Since 2021, the Public Integrity System of the Federal Executive Branch (*Sistema de Integridade Pública do Poder Executivo Federal*, SIPEF) further institutionalises and strengthens the Integrity Programmes and, with them, the requirement to ensure effective integrity risk management. This report reviews the methodology for identifying and assessing integrity risks in Brazil and provides concrete recommendations for strengthening the current approach.

Main findings

In 2018, the Office of the Comptroller General of the Union (CGU), central organ of the SIPEF, issued a Practical Guide to Integrity Risk Management to support federal entities. The document raises awareness of integrity risk management and provides guidance on its implementation, including concrete "how-to" steps as well as insights on generic integrity risks and cases. Within federal entities, the Integrity Management Units (UGI) play a crucial role in co-ordinating and supporting integrity risk management, as a "second line of defence".

Despite this relatively sound integrity risk management framework, Brazil is still facing significant implementation challenges:

- While some public entities are more advanced than others, most public entities in the Brazil federal executive are still at an early stage when it comes to mainstreaming integrity risk management.
- A major challenge concerns the difficulty of enabling a culture of public integrity that goes beyond a traditional compliance-based approach to encompass a context-dependent and risk-based approach.
- A lack of support from senior management has been identified as one of the main difficulties faced by the UGIs. Furthermore, only a small part of the work of UGIs is focused on advising and training staff on integrity issues, while there is a significant need to intensify training on these topics. Finally, there is a lack of public resources specifically assigned to integrity risk management, which prevents adequate investment in capacity-building and expanding public integrity-related activities.
- While IT tools could help public entities properly manage integrity risks, only very few of them currently use the tools available. In addition, the tools are mostly used on an *ad hoc* basis for

detection and investigative purposes, rather than being used systematically to anticipate critical events and strengthen public integrity.

Main recommendations

Overall, the challenges identified reinforce the need to continue improving integrity risk management in the Brazilian federal administration. Brazil could consider strengthening the current methodology for identifying and assessing integrity risks by working in three main areas that complement and build on one another.

- First, applying behavioural insights raise awareness of cognitive biases in judgement and help public managers better understand, identify and assess integrity risks. In essence, the idea is to make integrity risk management less sensitive, more intuitive and less complex. Brazil could incorporate such behaviourally inspired guidance into an IT tool to support public managers in taking better decisions.
- Second, Brazil could build on the significant progress made in recent years with data analytics tools such as “ALICE” or “FARO” to move beyond detection and investigation to develop solutions that support integrity risk management in federal entities based on predictive models. To do so, CGU could develop a strategy and action plan for using data and enhancing analytics.
- Third, it is essential to continue developing capacities for integrity risk management. This includes ensuring organisational support, staff training, sharing of best practices and providing *ad hoc* guidance on areas such as generic integrity risks, risk assessment methodologies, or data and IT literacy. This can best be achieved by working through the UGI and by training selected public managers to lead a change towards an integrity risk management culture.

1 Integrity risk management in Brazil's federal executive

Risk management supports public sector organisations in achieving their mandate and a wide range of policy goals and objectives. Integrity risk management in particular is at the heart of ensuring and promoting public integrity in an efficient and effective manner. In Brazil, the Office of the Comptroller General of the Union (CGU) leads integrity risk management and provides support and methodological guidance to public entities of the federal executive. In general, the CGU's integrity risk management framework is aligned with international standards. However, the implementation of the framework is uneven across the administration, with varying levels of maturity and several challenges remain in promoting a culture of risk management.

Integrity risk management: The foundation for efficient integrity policies

Risk management supports public sector organisations in achieving their mandate and a wide range of policy goals and objectives (OECD, 2020[1]). Risks need to be identified, analysed and adequately managed. Among the variety of risks that can affect a public organisation, corruption, fraud and other unethical practices can undermine public integrity and threaten the achievement of the public policy goals and objectives. Furthermore, they impede an efficient use of public resources and are further undermining public trust in institutions.

In light of this, the OECD Recommendation on Public Integrity puts risk management at the heart of any strategy or approach to ensure and promote public integrity. The Recommendations calls on adherents to "apply an internal control and risk management framework to safeguard integrity in public sector organisations" (OECD, 2017[2]), echoing various international standards and guidance. For instance, several organisations have developed international frameworks or guidance for risk management in the public sector, such as the Committee of Sponsoring Organizations of the Treadway Commission (COSO), the International Organisation for Supreme Audit Institutions (INTOSAI), the Institute for International Auditors (IIA) and the International Organisation for Standardization (ISO), among others.

In particular, countries should aim at ensuring a control environment with clear objectives that demonstrate managers' commitment to public integrity and public-service values and that provides a reasonable level of assurance of an organisation's efficiency, performance and compliance with laws and practices. They should further ensure a strategic approach to risk management that includes assessing risks to public integrity, thereby addressing control weaknesses (including building warning signals into critical processes), establishing an efficient monitoring and quality assurance mechanism for the risk management system and effectively strengthening the prevention of integrity violations.

In the public sector, normative and policy frameworks for risk management often align with international standards; however, implementation challenges typically persist. Ideally, public managers should identify and manage the risks arising in the processes and areas of their responsibility. An adequate understanding and assimilation of risk management allows to use continuously the information on risks to make management decisions by the administration. In addition, risk assessment mechanisms should be incorporated within a cyclical process where not only risks, but also methodological issues are revised and updated by incorporating new empirical evidence (OECD, 2018[3]).

The value of risk management is not always clear to public managers, however. For example, understanding why risk management matters requires, in the first place, a clear understanding of the values and objectives of the public function that is exercised. The lack of clear objectives and performance culture often observed in the public sector together with weak accountability and the difficulty to quantify both impact and productivity of the public sector, may undermine such a clear understanding. A public manager that is not held accountable for achieving objectives, or if these objectives are not clearly specified, may not feel the pressure to deliver and thus to identify and manage the risks that could undermine their achievement. In addition to the often unclear incentives, public managers may lack capacities and knowledge on how to manage risks and/or may lack support from their organisation.

In Latin America, similar to other regions, an OECD reported identified three main obstacles to achieving an effective risk management system (OECD, 2019[4]):

- Public managers are unaware of, or lack knowledge about, the standards, policies or guidelines on risk management.
- Public managers do not have a clear understanding about the concept of "risks" and about the processes and utility of risk management.
- Public managers believe that risk management is a function to be undertaken by someone else and do not see this as a task that belongs to their own management function.

While these challenges apply for risk management in general, they are also particularly relevant for managing integrity risks, where challenges may be even more severe and more complex given that it is a sensitive and complex topic. On the one hand, some unethical practices may be rationalised by public officials as legitimate or as normal ("that's how things work here") or these unethical practices may not even be perceived anymore as a problem. On the other hand, some fraud and corruption risks may be difficult to identify for public officials if they lack an understanding of complex fraud and corruption schemes or are simply unaware of the many different practices related to corruption. They may also be reluctant to speak about corruption and fraud risks when they are equalling risks with actual occurrence or feel that they are "talking bad" about their unit or themselves.

This OECD report reviews the current methodology for assessing integrity risks in the Brazilian Federal executive branch and provides avenues for modernising and strengthening the current methodology. The remainder of this chapter presents the integrity risk management framework and the challenges faced in its implementation. While the normative underpinning and guidance for integrity risk management will be analysed in detail in the forthcoming OECD Integrity Review of Brazil (OECD, forthcoming[5]), Chapter 2 focuses on three concrete avenues to strengthen and modernise the current approach by acknowledging and addressing cognitive and social barriers to an effective integrity risk management, by leveraging ongoing efforts to improve the use of data and data analytics for the purpose of preventing integrity violations and, finally, by strengthening the organisational support to integrity risk management in public entities of the federal executive.

Integrity risk management in Brazil's federal executive branch

Brazil has a solid integrity risk management framework that is aligned with relevant international standards and provides guidance to public managers

In Brazil's federal executive branch, the Joint Normative Instruction No. 01/2016 established the creation and improvement of internal management controls, governance and risk management. In the following year, integrity risk management became mandatory for all federal public entities with Decree 9203/2017. Integrity risk management is a key element of the Integrity Programmes and the Integrity Plans that have been established since 2017 in all 186 entities of the Federal executive to prevent, detect, punish and remediate fraud, corruption and other unethical practices. In 2021, the creation of the Public Integrity System of the Federal Executive Branch (*Sistema de Integridade Pública do Poder Executivo Federal*, SIPEF) through Decree 10756/2021 further institutionalises and strengthens the Integrity Programmes and with them the requirement to ensure an effective integrity risk management (Box 1.1).

Box 1.1. The Public Integrity System (SIPEF) in Brazil's Federal Executive

The Office of the Comptroller General of the Union (*Controladoria Geral da União*, CGU) is the internal control body of the Federal Government and, since its creation in 2001, has been a core element of the federal government's strategy to enhance integrity and prevent corruption in Brazil (OECD, 2012[6]).

In particular, the CGU is responsible for co-ordinating the implementation of Integrity Programmes to prevent, detect, punish and remediate corruption, fraud, illicit acts and violations of the standards of conduct in all public entities of the Federal Executive (Decree 9203/2017, subsequently regulated through Ordinance 1089/2018 and Ordinance 57/2019).

Integrity Programmes have to be developed along a number the following axes:

- Commitment and support from senior management.
- Existence of a unit responsible for implementation in the organ or entity.
- Analysis, evaluation and management of risks associated with integrity.
- Monitoring of the elements of the Integrity Programme.

Integrity Programmes aim to ensure that in every federal entities all internal units responsible for integrity-related activities and areas work together in co-ordination to ensure integrity and minimise integrity risks. The Integrity Management Unit (*Unidade de Gestão da Integridade*, UGI) are responsible, within each institution, to co-ordinate the development of the internal Integrity Plan of the public entity, as well as its subsequent implementation, monitoring and evaluation. Senior management need to approve these Integrity Plans, which set out the integrity measures and an action plan for their implementation.

The Public Integrity System of the Federal Executive Branch (SIPEF), established in July 2021 through Decree 10756/2021, further formalises and strengthens the normative basis for the Integrity Programmes and the UGI, with the CGU as its central organ (OECD, 2021[7]). The SIPEF establishes the UGI as the systems' responsible sectorial units, expanding their functions and responsibilities. These responsibilities could be summarised as articulating different integrity efforts within the entity, but also include providing guidance, training and support on matters related to public integrity and integrity risk management.

Source: (OECD, 2012[6]) and (OECD, 2021[7]).

The Office of the Comptroller General of the Union (*Controladoria Geral da União*, CGU) first defined integrity risks as a "vulnerability that could favour or facilitate the occurrence of corruption, fraud, illicit acts and/or violations of the standards of ethics and conduct, which in turn could compromise the aims of the institution" (CGU Ordinance 57/2019). Recently, with the SIPEF, the definition of an integrity risk was revised to the "possibility of an event of corruption, fraud, irregularity or ethical or conduct deviation that may impact the achievement of institutional objectives" (Decree 10756/2021). The CGU emphasises that integrity risk management permeates across the federal government, including different functions (e.g. human resource management, public financial management, internal control and risk management and public procurement) and sectors (e.g. infrastructure, housing, health, education, taxation and customs).

In 2018, the CGU issued a *Practical Guide to Integrity Risk Management* to support federal entities (CGU, 2018[8]). The document provides guidance on the implementation of integrity risk management, raises awareness and delivers concrete "how-to" steps for implementation. The guide also reinforces the notion that managing integrity risks is the responsibility of public managers as risk owners. Specifically, it requires that managers should establish, monitor and improve risk management and internal control systems. This includes the identification, assessment, mitigation and monitoring of integrity risks that may affect the achievement of objectives when fulfilling the institutional mission of public entities.

In line with the OECD Recommendation on Public Integrity (2017), CGU's Guide shifts the focus of integrity policies towards a context-dependent, behavioural and risk-based approach. Its general nature enables federal public entities to adapt the methodology to specific contexts while ensuring a minimum of coherence across the federal administration. This means as well, for example, that if a public entity already has adopted a risk assessment methodology for other areas, it will be able to apply this methodology to the identification of integrity risks. In addition, the guide offers flexibility to continually improve the methodology while the institution gains maturity in its implementation.

The guide also invites going beyond the traditional anti-corruption approach based on compliance with the rules and reinforces the relevance of promoting an effective cultural change in the organisation. In this sense, CGU emphasises principles and aspects in the management of integrity risks, such as the commitment of senior management, the support for the engagement of different parts of the public entity and the capacity building in the field of public integrity.

Furthermore, the guide supports public managers in identifying integrity risks by providing a generic list of potential events that may hinder the realisation of organisational objectives ("transversal integrity risks") and by providing methodological tools. Public entities are invited to employ different methodologies to collect information and identify integrity risks, such as analysing information that already exists within the organisation (Box 1.1), taking advantage of public servants' experiences and skills, exchanging experiences with similar organisations or analysing scenarios. Choosing the best approach will depend on the organisations' maturity and the available human and financial resources. For example, as one possible tool amongst others, the Guide suggests the use of brainstorming workshops, to encourage key actors to meet and share viewpoints to facilitate risk identification.

Box 1.2. The use of data on past disciplinary proceedings to identify integrity risks by the Brazilian Federal Police

The Brazilian Federal Police's integrity risk assessment illustrates one of the methodologies to conduct the identification of integrity risks using data on past cases. Indeed, the Federal Police kicked off the risk assessment process with the qualitative analysis of the 2 384 disciplinary proceedings (*Processo Administrativo Disciplinar*, PAD) that led to dismissals, position removal and pension cancellation. The data was obtained from the Disciplinary Process Management System (CGU-PAD). Then, the Federal Police analysed only those PADs that imposed sanctions and selected a sample, excluding the procedures associated with non-expulsive sanctions (e.g. warnings) and those that did not involve any corruption act, totalling 40 PADs. During this process, transversal risks were identified, such as illicit enrichment, bribery to leak privileged information, undue access to consultation systems and inspection fraud. The identified integrity risks were then categorised into four main events: personal advantage, leaking of information, privileged services trading and fraud. While in this case the Brazilian Federal Police adopted a methodology based on past disciplinary procedures, the CGU emphasises that organisations should not focus solely on past on events (CGU, 2018[9]).

Source: OECD, based on information provided by the CGU.

Principally, the CGU guide provides the methodology for assessing integrity risks. To do so, it follows the standard approach of categorising a risk according to its likelihood and impact and emphasises several ways to estimate and present both dimensions of an integrity risk, depending on its accuracy and complexity. In particular, the CGU Guide encourages each organisation to adopt impact and probability rating scales to build a heat map, depending on the aspired complexity. Organisations with less mature integrity risk management activities, for instance, can adopt basic methodologies, such as a 4x4 matrix (four probability levels and four impact levels) as shown in Table 1.1 below. Accordingly, for each catalogued integrity risk, the organisation must score the possibility of its occurrence (probability) and the severity of the possible consequences (impact). This process sets the ground for analysing the most appropriate measures to address the risks according to their severity.

Table 1.1. Integrity risk matrix with 4x4 levels

Metrics	Probability	Impact
1 – Very low	The event has a very low probability of occurring	Insignificant consequences if the event occurs
2 – Low	The event rarely occurs	Minor consequences on secondary processes and activities
3 – Medium	The event has already occurred a few times and may reoccur	Relevant consequences on secondary processes and activities or minor consequences on priority processes and activities
4 – High	The event has occurred repeatedly and will likely reoccur many times	Relevant consequences on priority processes and activities

Source: (CGU, 2018[8]).

In addition to identifying, describing and rating the risks, the guide also requires that organisations point out the most significant causes and consequences associated with this potential event. Identifying causes makes it possible to grasp the reasons or circumstances that are more likely to encourage, cause or allow any misconduct that violates public integrity. Mapping the consequences, in turn, enables a better understanding of how the integrity risks can affect the objectives of the organisation (CGU, 2018[9])

Finally, the CGU guide provides orientation on how to use the information obtained from the risk assessment and the heat map to introduce efficient and effective measures to mitigate those risks. When

developing the integrity plans, the guide recommends that public entities should focus on the most relevant integrity risks to be managed, that is, those with both the most significant impact and probability within a risk level previously defined by senior management. Public entities should prioritise integrity risks that exceed their risk tolerance ("*apetite a riscos*"). According to the guide, the integrity plans then should identify and promote the implementation of measures to avoid, mitigate or transfer the most relevant, prioritised integrity risks, ensuring that appropriate responses are timely. Based on the priorities established in the heat map and the risk tolerance level, the entity should verify already existing measures and assess the need to improve or establish new strategies. Personnel training, transparency promotion, social control and reducing the level of discretion of decision makers in sensitive processes are some of the measures recommended by the CGU guide to address integrity risks (CGU, 2018[8]). Several other actions can be taken, depending on the specific risks of each organisation and the availability of resource. In addition, the guide emphasises that it is essential to adapt the measures to the actual needs of the organisation to help achieve its objectives, instead of generating unnecessary bureaucracy and slowing down processes.

The identification, assessment and mitigation of integrity risks is a crucial step for the approval of the integrity plan. As pointed out by the CGU, carrying out integrity risk identification and assessment prior to implementing the integrity programme helps to identify processes and areas that are more susceptible to corruption and enables the entity to act timely and adjust to new risks over time (CGU, 2018[9]).

Institutionally, within federal entities, the Integrity Management Units (*Unidades de Gestão da Integridade*, UGI) are playing a crucial role in co-ordinating and supporting integrity risk management, as a unit of the second line of defence. The UGI are mandatory and established in all entities of the Federal executive. They co-ordinate the development of the Integrity Plan of the entity and the subsequent implementation, monitoring and evaluation of the plan. With the Public Integrity System of the Federal Executive Branch (SIPEF), there is an opportunity to further strengthen the UGI to ensure they can deliver on the key role they are playing as sectorial units of the SIPEF (OECD, 2021[7]).

Despite the relatively sound integrity risk management framework, Brazil is still facing significant implementation challenges

In Brazil, capacity for risk management has long been a challenge in the government. In 2014, TCU conducted a survey in co-ordination with the Rui Barbosa Institute, the Association of Members of the Brazilian Courts of Accounts (*Associação dos Membros dos Tribunais de Contas do* Brasil*,* ATRICON), and 28 subnational audit entities, which highlighted the systemic need for improved risk management and control in government. Specifically, they assessed the maturity of risk management based on a set of criteria and identified inefficiencies in risk management in public sector entities. Out of the 380 federal public entities surveyed, 304 (80%) at the time were considered at an early stage of risk management (i.e. non-existent or insufficient capacity) (TCU, 2014[10]). Ensuring an effective implementation remains one of the key issues facing the Brazilian government concerning integrity risk management, and in general, ensuring effective accountability.

As noted above, implementing risk management in the public sector is a challenge, but implementing *integrity* risk management perhaps even more (OECD, 2019[4]). Many countries struggle with applying the conceptual frameworks in day-to-day practice and promoting a culture of integrity risk management in public entities. Brazil is not an exception. OECD fact-finding through a questionnaire, an online focus group with UGI and CGU as well as several interviews conducted with public officials evidenced that despite the normative framework and the available guidance, integrity risk management is still at an early stage. While there is a degree of heterogeneity with respect to the maturity of integrity risk management across the federal administration, with some public entities being more advanced than others, there is an overarching acknowledgement that there are still important implementation challenges in the majority of public entities in the Brazil federal executive.

One of the major challenges related to strengthening integrity risk management in Brazil concerns the difficulty of consolidating a culture of public integrity that goes beyond the traditional legalistic view and begins to encompass a context-dependent and risk-based approach. The results obtained from the focus group conducted by the OECD demonstrate that the compliance culture is still widespread among federal public entities and that there is a strong resistance to change among civil servants.

In addition, it is essential to have the support of senior managers and invest in employee training. In practice, however, the answers to the OECD questionnaire indicate that the lack of support from senior management is one of the main difficulties faced by the UGIs in carrying out their work and supporting integrity risk assessments. Furthermore, despite the relevance of investing in capacity building, the results of the fact-finding conducted by the OECD reveals that currently only a minimal part of the work of UGIs is focused on advising and training staff on integrity issues. Additionally, there is a significant need to intensify training on specific public integrity topics in areas that carry out activities related to this matter.

Other challenges relate to obstacles that have been preventing the effective institutionalisation of integrity risk management in the Brazilian federal executive. First, there is a lack of public resources specifically assigned to this agenda, which ends up preventing adequate investment in building capacities and in the expansion of public integrity-related activities. According to the results of the OECD questionnaire, 93% (28) of the UGIs that responded did not have their own budget at that time. This means that activities related to integrity are currently often subject to the availability of public resources allocated to the other non-integrity related activities of the UGI. Second, there is insufficiency of skilled labour fully dedicated to the management of integrity risks. In this regard, the OECD focus group drew attention to the fact that the public managers responsible for carrying out integrity risk management often work at the limit of their capabilities, having to perform other duties. In turn, the UGIs could provide support to public managers but generally do not have a staff with exclusive dedication and properly trained to deal with integrity risk management (OECD, 2021[7]). These issues explain why integrity risk management is not yet widely implemented among federal government entities, which leads to incomplete integrity plans, unfinished risk analyses and difficulties in establishing effective detection systems.

In addition, while IT tools can help public entities to properly identify integrity risks, assess them and assist public managers in the decision-making process, such tools are currently used only in very few public entities. Even then, these tools are mostly used for detection and investigative purposes, rather than being used to anticipate critical events and strengthen public integrity. Examples of these tools are: ALICE (*Analisador de Licitações, Contratos e Editais*, Bids, Contracts and Public Notices Analyser) and FARO (*Ferramenta de Análise de Riscos de Ouvidoria*, Instrument for Risk Analysis of incoming report to the Ombudsman). The CGU and, for the case of ALICE, also the Federal Court of Accounts (*Tribunal de Contas da União*, TCU), use these tools to support investigation of suspicious events. ALICE focuses on public procurement, FARO supports the analysis of complaints directed to the federal ombudsman. These IT tools, and how Brazil could build on them to strengthen integrity risk management, will be analysed in more detail in Chapter 2.

AGATHA, a tool developed by the former Ministry of Planning, Development and Management (MP) aims to support the risk management and internal controls system. This tool was designed to help managers to assess internal and external strengths, weaknesses, opportunities and threats (SWOT analysis) and to identify, assess and guide critical risk analysis to positively impact the achievement of the public entities' objectives as requested by Decree 9 203/17. However, in practice, this tool is not being widely adopted, despite being available under a free license. For example, among the UGIs that responded to the OECD questionnaire, only 10% (3) are currently using AGATHA and one entity is considering its use. A few other units are in the process of implementing this tool and some point to the urgent need for training and clearer guidance on how to use AGATHA. Interviews carried out by the OECD to understand the reasons why AGATHA is not being used more systematically indicated that the tool is not user-friendly and is limited in terms of analytical support, offering only a heat map to facilitate analysis.

Overall, the points raised above reinforce the need to continue improving the maturity of integrity risk management in the Brazilian federal administration. Not at least, the Covid-19 outbreak imposed several additional challenges to countries, including Brazil, expanding public spending, exacerbating their financial situation, blurring decision-making processes and obstructing social control. As reported during the fact-finding, public entities in Brazil have experienced several challenges to carrying out their work under these new circumstances. In addition, it was reported that the public integrity agenda lost importance because of the crisis among some public entities, which reflected in exacerbating the budget constraints to deal with this matter.

Unfortunately, a recent survey on ethics and corruption in the Brazilian federal public service reveals that, during the Covid-19 crisis, there has been an increase in public managers' perceptions of corrupt acts, such as political interference in the decision-making process and limited transparency and accountability of decisions concerning public procurement and contracting (Ortega Nieto et al., 2021[11]). Hence, in a context of crisis, integrity risk management becomes even more relevant to guide efficient and effective integrity policies.

Nonetheless, it is noteworthy that, despite the challenges experienced in some public entities during the current crisis, the establishment of the SIPEF in 2021 constitutes a milestone which reinforces that Brazil is on the right track to consolidating the integrity agenda in the federal executive. However, this new system still requires to be reinforced to achieve its goal of promoting cultures of integrity risk management in the federal administration (OECD, 2021[7]). Based on the analysis of the current situation, the following chapter provides concrete avenues to continue strengthening the culture of public integrity and integrity risk management. The recommendations presented in the next chapter will be complemented by the OECD Integrity Review of Brazil (OECD, forthcoming[5]), which will provide a more systemic analysis of the integrity risk management and control framework in Brazil.

2 Three avenues to strengthen integrity risk assessments in Brazil's federal executive

This chapter provides three concrete avenues to strengthening and modernising the approach for identifying and assessing integrity risks in Brazil's federal executive. First, it recommends to acknowledge and address cognitive and social barriers to improve the accuracy of human judgment and to foster an integrity risk management culture. Second, ongoing efforts to improve the use of data and data analytics could be leveraged to support integrity risk management. Third, the Public Integrity System of the Federal Executive Branch (SIPEF) offers an opportunity to promote leadership and reinforce the organisational support to integrity risk management in public entities, in particular through the Integrity Management Units (UGI).

Chapter 1 described and analysed the main challenges Brazil is facing in ensuring an effective implementation of the current integrity risk management framework and in particular in promoting a risk management culture throughout the federal executive branch. At the same time, integrity risk management becomes even more relevant in times of crisis, by ensuring not only effective but also efficient integrity policies and thus value for money.

As such, Brazil could consider strengthening the current methodology and approach by working along three main avenues that complement and build on one another:

1. Demystify and simplify qualitative integrity risk assessments.
2. Advance integrity risk management through the use of data and analytics.
3. Strengthen the organisational support for integrity risk management and empower public managers.

Demystify and simplify qualitative integrity risk assessments

Behavioural barriers and biases in integrity risk management

The risk-based approach is fundamental to the OECD Recommendation on Public Integrity. The idea can be found throughout the Recommendation, which emphasises that risks analysis should guide the measures taken to mitigate these integrity risks, so they are proportionate, efficient and effective. However, it is easy to forget that the achievement of this goal rests, amongst others, upon three fundamental key steps: the accurate identification, assessment and mitigation of risks that could affect the achievement of the mandate and objectives of a public entity (Figure 2.1). In addition, integrity risk management should be clearly communicated, monitored and evaluated to ensure an effective implementation and learning over time. Each of these steps needs to be effective to reach the overall goal of integrity risk management and it is key to identify and understand potential challenges and problems.

Figure 2.1. Three steps of integrity risk assessment management

While the CGU guide described in Chapter 1 provides orientation on all the three steps and emphasises the need to promote integrity risk management cultures in public entities, it only provides limited guidance on how this could concretely be achieved. Of course, there are a wide variety of aspects related, for example, to normative frameworks or available capacities that are fundamental to set a strong foundation for effective integrity risk management. These will be analysed in more detail in the forthcoming OECD Integrity Review of Brazil (OECD, forthcoming[5]). This section looks into some behavioural barriers and biases that can undermine integrity risk management in each of the three steps outlined in Figure 2.1, where human judgement and experience continues and will continue to provide relevant information. Indeed, the CGU guide currently lacks an analysis of such behavioural dimensions.

Applying behavioural insights can help in uncovering these cognitive biases and systematic errors in judgement to inform strategies to support public managers (risk owners) to improve the understanding, identification and assessment of risks. In turn, this can lead to more targeted integrity measures and an internal control system that is more resilient to fraud and corruption and, in the end, contributes to establishing an integrity risk management culture in public entities.

Indeed, human beings are subject to several biases that make it difficult for them to identify and assess the likelihood of occurrence and potential impact of a given risk event. Despite the use of methodologies that mimic objective assessments, the identification and the assessment of risks will always have a subjective component (Slovic, 1999[12]). The following aspects can affect the judgement of the public officials participating in integrity risk assessments, particularly in qualitative risk assessments such as those promoted in the CGU's guidance:

- The concept of "risk", and risk tolerance, is often misunderstood or difficult to define and communicate, particularly in the context of integrity risk management where a zero-tolerance is promoted in political rhetoric. In addition, unconscious rationalisation of unethical practices or the sensitivity that goes along with integrity violations may undermine the identification of relevant risk events. On the one hand, the task of identifying integrity risks may trigger discomfort or even fear. Public officials may perceive that identifying risks in processes under their responsibility corresponds de facto to an evaluation of their own integrity or the integrity of their teams. They confuse the risk of integrity violations with their actual occurrence. On the other hand, while public officials often do not understand the value added in identifying and managing risks, they may very well perceive potential costs for them. Public officials may then be *unwilling* to identify integrity risks, as they may perceive such an exercise as indicating weaknesses in their units and processes with potential consequences. For instance, officials may be reluctant to draw the attention of investigation or audit units, potentially creating additional work and stress.
- To identify more specific integrity risks, a detailed knowledge of the sector, the organisation and the processes is needed. As such, it can be useful to engage managers and frontline employees. They are directly responsible for operations or service delivery across the organisation and can improve risk identification by providing different perspectives and to validate the results of the risk mapping (OECD, 2020[1]). Following this logic, the CGU guide recommends the use of risk workshops, which are similar to brainstorming sessions, to identify risks and take into account different perspectives and experiences by involving public employees (CGU, 2018[8]). However, several behavioural insights show that brainstorming sessions are subject to social dynamics that may compromise the identification of risks. For instance, instead of correcting errors made by individuals of a group, a group can amplify these errors. Groups could just follow the ideas of those who spoke first, they could polarise around extreme ideas or focus on what everybody already knows instead of taking into account critical information of individuals that may not want to speak up (Sunstein and Hastie, 2014[13]).
- Finally, the assessment of identified risks can be biased as well. Several studies find that humans are quite bad in thinking statistically and as such may face problems in assessing correctly the likelihood of risks (Kahneman and Tversky, 1982[14]; Kahneman and Tversky, 1972[15]). To deal with uncertainty and assess probabilities, humans tend to use heuristics (Tversky and Kahneman, 2007[16]). While these heuristics are cost-efficient, they often lead to biased judgments. For instance, humans tend to confuse plausibility with probability. However, a risk that seems plausible or has the most coherent narrative is not necessarily the most likely to occur. A typical factor that can bias our estimated probability is the base-rate fallacy. When asked for integrity violations in a given procedure, humans will imagine or remember how many times a violation occurred, but usually do not take into consideration how many times the procedure took place without any integrity violation. In addition, risk events that tend to affect us emotionally or that we have directly experienced in the past, are likely to trigger stronger feelings and make us believe they are more

likely (Loewenstein et al., 2001[17]). Availability of information or salience of a topic may also influence our estimates. A strong media coverage on corruption cases, for example, could skew our perception towards overestimating the likelihood of occurrence of certain integrity risks. Finally, different worldviews and beliefs can lead to very disparate risk ratings with the result that the risk matrix has little or no benefit to manage risk effectively and rationally (Ball and Watt, 2013[18]).

Even if integrity risks have been reasonably well identified and assessed, through qualitative or quantitative techniques, behavioural barriers and biases may undermine taking the correct decisions with respect to the way to deal with these risks and thus affect an effective risk mitigation. Indeed, public managers that have to act based on the risk information available can either be prone to inaction or over-reaction.

- On the one hand, overconfidence or blindness to vulnerabilities could lead to preventive measures that are too weak. The already mentioned blindness to some unethical practices and the sensitivity related to integrity risks coupled with potential misunderstanding of risk vs. occurrence could lead public managers to prefer closing their eyes on integrity risks instead of taking actions, for example to avoid being in the focus of attention and potential stress, stigma or additional work.
- On the other hand, overly risk averse public managers and/or contexts where corruption scandals are widely covered in the media and are driving reactions from citizens and opposition parties, could lead to measures that are too strict ("overshooting"). Loss aversion is indeed a widely researched and established behavioural insight (Kahneman and Tversky, 1979[19]). The costs of facing a corruption scandal in an entity could seem prohibitive to senior management and could thus lead to extreme measures. However, it is important to bear in mind that anti-corruption measures come along with costs too (Falk and Kosfeld, 2006[20]; OECD, 2018[21]; Schulze and Frank, 2003[22]). These costs are related to trade-offs with flexibility and innovation, to psychological costs due to the signal of distrust that is sent to public servants and to the risk of crowding out intrinsic motivation to honesty.

To address behavioural biases, the CGU could review the current integrity risk assessment methodology and provide technological support to public managers throughout the process

As emphasised in Chapter 1, there a several challenges to implement an integrity risk management culture. These are related to capacity constraints (knowledge about integrity risks) and time constraints (competing priorities). In addition, the previous section emphasised that behavioural biases may exacerbate the challenge of establishing cultures of integrity risk management. While the CGU guide recognises some of these challenges, it does not provide guidance and support on how to address them concretely. In this case, applying behavioural insights means acknowledging and addressing the potential problems identified in the previous section. Concisely, the idea is to make integrity risk management less sensitive, more intuitive and less complex.

In particular, the CGU could consider to follow advice from behavioural insights by the following strategies or measures:

- *Support identification of integrity risks by overcoming misunderstandings and demystifying integrity risks.* The willingness to identify integrity risks in the first place is key for the outcome of integrity risk management. The CGU and the UGI should therefore continue and perhaps intensify efforts to explain the concepts of integrity and risks. In essence, it is key that public managers understand that integrity risk management looks at the integrity of positions and processes, not at their own personal integrity. As much as possible, communication needs to uncouple risk identification from specific cases. A strategy could be to start with a thought experiment along the following lines: "Imagine you leave your current position and want to ensure that whoever comes next cannot abuse the position and the processes under his or her responsibility." Communication should also

aim at "normalising" integrity risk management as far as possible. Managers should become aware that integrity risk management ultimately supports the achievement of institutional goals and objectives through better decision making, more targeted allocation of resources and avoidance of reputational damage.

- *Support identification of integrity risks by simplifying the methodology and providing intuitive guidance.* Even though the current integrity risk management framework in Brazil corresponds to international standards and practice, the fact-finding during this project evidenced that it is perceived as complicated and requiring specific skills. Details matter, but integrity risks are often well-known and could be dealt with in a more generic way. In essence, taking into account the current maturity of integrity risk management in the Brazilian government, there are benefits in simplifying approaches, identifying small wins and resisting the urge for overly sophisticated approaches to assessing integrity risks, while being aware of biases and pitfalls of qualitative risk assessments, as discussed.
- *Address problematic group dynamics to avoid biases in the identification and assessment of integrity risks.* Acknowledging issues arising in brainstorming sessions can help in counterbalancing these when implementing group work. As such, the CGU could adopt techniques to avoid typical pitfalls in brainstorming and groupthink (Sunstein and Hastie, 2015[23]). For example, adapting it to integrity risk identification, Brazil could consider the methodology developed in the UK where participants silently (but not anonymously) contribute to a single online document at once (Box 2.1). Similarly, integrity risks could be identified by a group working jointly on an online joint document. When efforts mature, Brazil could also explore the integration of qualitative and quantitative insights for triangulating risks in key sectors and validating manager's perceptions of risk likelihood and impact, based on historical data when available.
- *Support a more adequate assessment of integrity risks and use of the information obtained.* Along the process, reminders or nudges could aim at making salient typical biases in human assessments of risk events. Essentially, the idea is nudging public officials involved in risk assessment to move towards a more reflective use of the information and to be less subject to the biases described in the previous section. Arguably, even simple reminders of potential biases could lead public managers to switch from an intuitive, largely unconscious way of thinking, that avoid efforts but is subject to biases (thinking fast, or "system 1"), to a more rational and conscious thought process (thinking slow, or "system 2") (Kahneman, 2013[24]).

Box 2.1. Behavioural insights to empower employees at a collective level in the United Kingdom

In the United Kingdom, the Behavioural Insights Team (BIT) has developed a "ThinkGroup" process, where participants silently (but not anonymously) contribute to a single online document at once. The BIT instituted this tool to enable participants to both interact and pursue their own train of thought in order to make brainstorming more effective (Hallsworth et al., 2018[25]).

On the online document, contributors can choose the ideas they want to develop or respond to, based on other contributors' inputs. This tool represents a useful alternative or complement to traditional in-person brainstorming discussions. In a traditional collective brainstorming meeting, the group's attention focuses on one idea at a time, preventing individuals from pursuing their own train of thought on different aspects of the discussion.

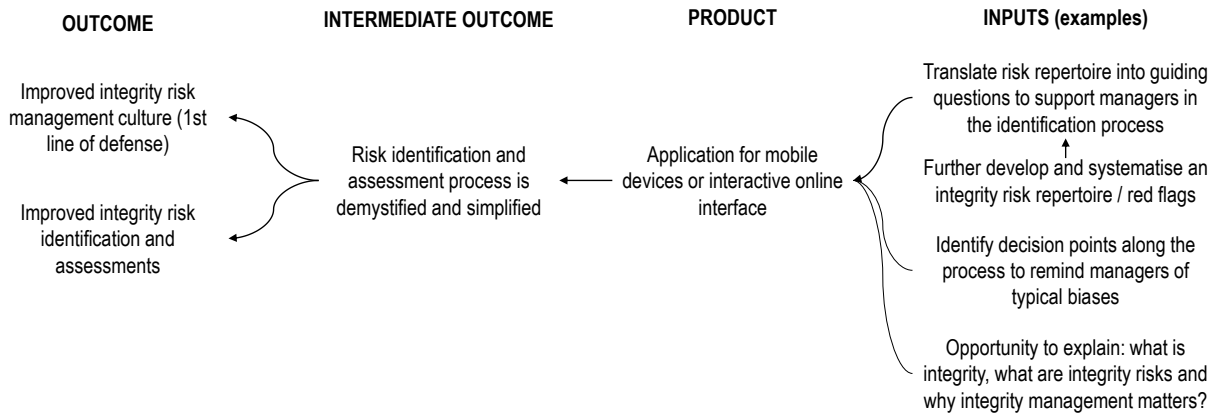
Such a tool can also improve openness in an organisation, by enabling employees to share ideas or concerns. Being a less confrontational and less direct form of exchange, using an online document might appear less intimidating and give participants time to properly formulate ideas and concerns.

Source: (Hallsworth et al., 2018[25]).

Finally, IT tools could incorporate some of these behaviourally inspired recommendations and contribute to support public managers throughout the process. As mentioned in Chapter 1, AGATHA is currently not user friendly enough to make a difference and, for these reasons, has not been widely adopted in the Brazilian public administration. Therefore, Brazil could consider reviewing and simplifying AGATHA. However, developing a new tool from scratch, in line with CGU guidance and behavioural insights, may be an easier solution. The resulting product supporting public managers could be an interface in an application for mobile devices and/or an online platform that guides the public managers through the process of integrity risk management. The tool would aim at reducing the inputs of public managers to a strict minimum and at the same time serving a pedagogical function by clarifying concepts related to integrity and risk management. To achieve this, the CGU could prepare automated guidance and information on the typical generic integrity risks in advance and incorporate these into the interface. The CGU already has started working on systematising such "transversal integrity risks", which could be used as a starting point. This work could be translated into guiding questions to support public managers and to walk them through the process of identifying an assessing integrity risks.

Such a user-friendly and simple interface could contribute to demystifying integrity risk management and help in overcoming typical misunderstandings and fears. Ultimately, such an interface could contribute to improving the quality of risk assessments and in promoting integrity risk management cultures in federal entities. The interface could be promoted through the UGI to ensure that all federal entities are on board. Over time, if a critical mass of participants are using the tool, the collected data could be aggregated centrally by the CGU to inform sectorial or regional risk maps. Figure 2.2 provides an overview of the theory of change underlying such an IT tool to support managers in integrity risk management.

Figure 2.2. Theory of change for an integrity risk management interface



Continue advancing integrity risk management through the use of data and analytics

The development of Information and Communication Systems has led to the generation of a significant volume of data in the public sector. Considering the human limitation in making sense of big amounts of information, governments around the world began to adopt digital strategies to take advantage of the profusion of data mushrooming over the past years, creating new opportunities for improving integrity risk management. Alongside the behavioural insights discussed in the previous section, data and analytics can further facilitate future iterations of CGU's efforts to manage and assess integrity risks (OECD, 2019[26]).

Indeed, using quantitative techniques and data analytics can help to identify potential fraud and corruption in a range of areas where governments tend to collect reliable and valid data by raising red flags (OECD, 2021[27]). Artificial intelligence (AI), including machine learning, has a rich history of applications for risk management, for example turning structured and unstructured data into insights for risk spotting and monitoring. Beyond raising red flags, analytics can inform integrity risk management to guide prevention. Predictive models can inform decision making and help managers react to risks before they materialise (OECD, 2021[28]). Methodologies for assessing risks based on AI or statistical analysis in general is only as good as the quality of the data available. Open and administrative data in areas such as public infrastructure, procurement, payroll, social services, health and employment services often are of sufficient quality for use and reuse.

Brazil has made significant steps towards leveraging data and analytics that can be used for integrity purposes

Applications of data and analytics to public integrity and risk mitigation are increasingly common in Latin America. Recent examples are Colombia and Mexico (OECD, 2021[28]; OECD, 2021[29]). Brazil as well has been an early adopter of analytics and a driver in the region in terms of their use for oversight and accountability. For instance, as mentioned in Chapter 1, ALICE (*Analisador de Licitações, Contratos e Editais*, Bids, Contracts and Public Notices Analyser) and FARO (*Ferramenta de Análise de Risco de Ouvidoria*, Instrument for Risk Analysis of incoming report to the Ombudsman) stand out in the context of supporting audits and investigations. ALICE is a Robotic Process Automation (RPA) tool that uses artificial intelligence (AI) to allow the continuous auditing of public procurement and contracting processes. ALICE has been deployed since 2015 by the CGU and, since 2016, by the Federal Court of Accounts of Brazil (*Tribunal de Contas da União*, TCU). The tool has contributed to fight corruption in public procurement. FARO is also an AI-based technology, adopted in 2021 by the Federal Ombudsman's Office (*Ouvidoria-*

Geral da União, OGU, which is part of CGU) to automate the investigation of the complaints sent by citizens through the Fala.BR online platform.

ALICE

In Brazil, the high volume of bids present major analytical challenges, considering that, based on information provided by Brazil, on average 357 notices are published each day. In addition, many tenders may be open for just a few weeks or even days. Consequently, auditors have to conduct risk assessments quickly before the contracts are signed, which in practice is nearly impossible. Aiming to overcome this challenge, the CGU and the TCU started deploying ALICE.

At the TCU, for example, this tool is programmed to access on a daily basis Comprasnet, the Brazilian Federal Public Procurement Portal (*Portal de Compras do Governo Federal*, https://www.gov.br/compras/pt-br), where data on public procurements at the federal level are saved. At CGU, ALICE is also programmed to retrieve data from Licitações-e and the daily federal publication register. Licitações-e is the procurement portal used by the Banco do Brasil, which is also shared with many state owned enterprises and local governments agencies. From the daily federal publication register, ALICE extracts information about bids that were waived and unenforced. According to information updated by the CGU, ALICE downloads the documents and data of all bids and carries out data matchings using 23 government data bases and 14 text analyses to detect signs of misbehaviour and risks in the tendering documents, such as bid rigging, competitiveness restriction, over-invoicing on prices and lacking important information in the public notice (Bemquerer Costa and Leitão Bastos, 2020[30]).

For example, ALICE analyses the “materiality factor”, which is an estimated risk value applied to the bidding notices. Since the bidding notices are saved in PDF, text is often not uniform. ALICE runs an algorithm that automatically obtains the monetary values of the bids from the PDFs and organises the data by applying a Random Forest classification method. According to the CGU, an agreement currently being negotiated with the Ministry of Economy will allow ALICE to directly access the correct monetary value of the bids. To detect irregularities in the tenders, ALICE also obtains relevant information from Comprasnet and saves it in a repository in a machine-readable format to later cross-reference with other datasets. The TCU has agreed with the Brazilian Federal Revenue to obtain confidential data regarding the bidder's Taxpayer Identification Number as a unique identifier to use for cross-referencing entities across databases and detecting anything that could be cause for ineligibility during the tendering phase.

ALICE has been generating a significant positive impact in strengthening the practice of identifying integrity risks in Brazil and fighting corruption in public procurement at the federal public administration. According to information provided by the CGU, in the first year that the ALICE came into use, more than 100 000 notices had been analysed and, between December 2018 and November 2019, 8 bids had been revoked, totalling approximately R$ 3.2 billion. In addition, 14 bids had been suspended due to signs of corruption uncovered by ALICE, totalling R$ 470 million. In 2021, 139 566 bids were assessed, 35 461 notices about risks where sent, 646 notices were analysed by auditors who opened 70 different audit engagements. According to the TCU activities report, in 2020, the amount of benefits arising from the analyses carried out through the ALICE system totalled more than R$ 194 million (TCU, 2021[31]).

ALICE constitutes a successful example of the use of data and analytics to identify red flags for potential corrupt acts and misbehaviour in procurement, as well as to enhance the efficiency of auditors' work. Two underlying success factors can be singled out:

- A decisive factor for obtaining valuable results in identifying corruption risks in public procurement was the support of senior management, which is deemed a key element in consolidating a culture of integrity. For instance, the use of ALICE innovated the way auditors tackle irregularities that are uncovered. The fact that auditors were promptly supported by the TCU Counsellors, who agreed to sign an ordinance validating a new workflow, enabled them to act in the most efficient way to address the risks and signs of corruption identified by this AI-based technology.

- To avoid overloading the auditors with information and address the human inability to process large amounts of data, both the CGU and the TCU have adopted two strategies to support auditors. First, ALICE sends daily emails with the bids' most important information and the alerts generated by the system, considering each area's main responsibilities, thereby enabling auditors to prioritise information to conduct their analyses. Second, a dashboard for auditors was created, which allows to apply different filters to target their search and where more detailed information about the analysis of bids conducted by ALICE and the irregularities can be found.

FARO

In Brazil, the Fala.BR online platform (falabr.cgu.gov.br) aims to address the challenge of examining the numerous complaints filed by citizens through the internet. Fala.BR is managed by the CGU to replace two different systems: the ombudsman system previously called e-Ouv and the access to information system formerly known as the e-SIC. It is an innovative platform that allows citizens to not only request information, but also to make complaints or claims against any federal body, express satisfaction or dissatisfaction for a service or programme, and provide suggestions for improving or simplifying public services (OECD, forthcoming[32]). At the federal level, the Federal Ombudsman's Office (OGU), a public entity directly linked to the CGU, is currently responsible for receiving these complaints. Throughout this process, the aptitude analysis is a fundamental step during which all materials referring to each of the complaints (their texts and attachments) are examined to verify if they meet the minimum requirements to be further explored by investigative units such as the disciplinary board or internal audit offices. To carry out this analysis, it is necessary to validate the information indicated in the texts and complement it with other external data.

A large number of complaints, together with the extensive volume of documents to be analysed, overburdens the OGU and prevents this entity from acting in a timely manner to investigate and take the necessary measures. Additionally, for a thorough understanding of what is pointed out by the citizens, it is generally necessary to take into consideration other information that is not presented in the text of the complaints. Therefore, to automate the examination process and promote greater efficiency in the aptitude analysis, the OGU started in 2021 to adopt FARO, an AI-based tool that supports the decision process of whether a complaint must be investigated or not. In addition to automating the processes of identification and extraction of certain variables from the texts of the complaints, this tool also enriches the input provided by citizens by correlating it with data from 57 external databases, thereby identifying new elements associated with the complaints.

The methodology applied by FARO to automate the complaints assessment of whether they are apt or not to be further examined includes five main steps (Paiva and Pereira, 2021[33]).

- First, in the conversion stage, this technology reads all the materials attached to the complaints, which usually come in different formats (e.g. images, spreadsheets, PDF, presentations etc.) and are often not machine-readable. These annexes are transformed into a text format and relevant information is extracted and linked to the original texts of the complaints.
- Second, FARO extracts relevant information from the texts of the complaints, such as the name of taxpayers and companies through the Individual Taxpayer Registry (*Cadastro de Pessoas Físicas*, CPF) and the National Register of Legal Entities (*Cadastro Nacional da Pessoas Jurídicas*, CNPJ), contract and agreement numbers, monetary values, as well as words or expressions considered relevant in the context of potential misconduct indicated by the complaints (e.g. fraud, corruption, overbilling). Once identified, all these elements are stored in a centralised database to be used throughout the investigation.
- Third, FARO carries out an expansion process, which consists of finding new information on the previously identified entities in one of the 57 external databases to validate their existence and to discover new elements and relationships. For instance, when a specific CNPJ is identified in the

text of a complaint, this variable is first cross-referenced with other databases to check if this is a valid CNPJ. Subsequently, other elements derived from this CNPJ are sought, such as the people listed as members of this entity.

- The fourth step consists of qualifying the entities identified in the previous phases. As an example, in the case of a CPF, it is possible to verify whether it belongs to a public servant or even if he/she receives benefits from social programmes.
- Finally, FARO conducts a data preparation, during which the information obtained in the previous steps is aggregated, thereby creating a centralised database that is used to train the model. Each complaint is represented by a set of structured data obtained from the original texts of the complaints (annexes included) as well as information derived from other sources.

As such, FARO proves to have significant potential as it allows deriving and including information that was not originally part of the complaints, and by improving the efficiency of the analysis of complaints. FARO reduces efforts to manually consult different documents and systems to assess whether it is worthwhile and possible to investigate the complaints forwarded to the OGU through Fala.BR platform.

According to data provided by the OGU, since the beginning of its operation in January 2020, FARO was responsible for the treatment of 5 361 complaints. 40% of reports were automatically classified by FARO as not fit for further investigation (obtaining a score under 30 points) and 8% automatically classified as having enough elements for initiating an investigation procedure (obtaining over 80 points). Thus, the ombudsman team was able to concentrate its efforts over the remaining 52% of the complaints, already pre scored and qualified with data from other government databases by FARO, to decide whether they had or not the elements needed by the investigative units.

CGU could develop a strategy and action plan to unlock the potential of existing data analytics initiatives for the prevention of integrity violations

Notwithstanding the advances of Brazil in the use of data and analytics and the benefits achieved so far, there are still some fundamental challenges to make the most of the use of data analytics in integrity risks management among the organisations of the Brazilian federal executive. To effectively embed the culture of integrity risk management in public entities and promote a preventive approach, it is necessary to implement strategies that go beyond the mere identification of red flags and investigative purposes.

For example, despite that ALICE helps identifying integrity risks in the bidding phase, this technology is implemented by the CGU and the TCU primarily to increase the efficiency of the auditors' work, enabling them to analyse a much larger quantity of bids and identifying red flags of corruption in the tendering phase. Indeed, even though both entities are advancing in the use of data science, have an excellent IT structure, are obtaining positive results and are expanding the use of ALICE to other courts of accounts at local levels (Project *Alice Nacional*), the tool is currently limited to investigative activities in public procurement (Bemquerer Costa and Leitão Bastos, 2020[30]). In addition, while public procurement is a major integrity risk area, it is not the only one, and Brazil could explore deepening the applications of analytics in other areas, such as the analysis of grants and subsidies or travel expenses, for example.

Therefore, the CGU could take advantage of the technical teams and the maturity already achieved in applying data science to develop a technological framework that supports integrity risk management in entities across the federal executive and is based fundamentally on predictive models. To do so, CGU could develop a strategy and action plan for using data and enhancing analytics that takes into account the specific context of integrity and anti-corruption in the federal public administration. In this exercise, a co-ordination and exchange of information between CGU and TCU could be considered.

Such a strategy and action plan should be based on:

- *Mapping databases that are relevant for assessing integrity risks.* Such a mapping includes a stocktaking of all databases potentially available for strengthening CGU's capacity to assess integrity risks. The mapping can build on the significant work achieved by the CGU and should not be purely descriptive, but should include an analysis of the quality, accessibility and relevance of the data for assessing integrity risks. In addition, it could include analysis of priority databases for further improving the data analytics strategy in the future.
- *Reviewing and carrying out a comparative analysis of analytics strategy and capacity.* The use of data and analytics relies on having strategies with clearly articulated objectives, as well as a range of pre-conditions and technical capacities. The CGU could assess these areas, including the data governance, data management and data skills available for assessing integrity risks. The analysis would provide a clear road map about areas for improvement to develop and implement the strategy and action plan.
- *Developing a data-driven integrity risk assessment model*. The model should reflect the maturity of the CGU based on different factors, including the creation of a platform that mainstreams several integrity-related databases, and be ambitious, state-of-the-art and theoretical sound. Leveraging on the experience with FARO, the CGU could use the latest in machine learning and artificial intelligence, as also used in Spain with OECD support (OECD, 2021[27]). Other techniques could include indicator-based risk scoring, for example. The objective of the model goes beyond the mere crossing of databases and aims at moving towards the use of analytics and AI-based tools that directly support integrity risk management, detecting patterns, making predictions and providing valuable insights.
- *Building capacities*. The strategy and action plan should identify and include objectives related to providing trainings and workshops to support the implementation of the risk model and addressing some of the challenges identified. These workshops are an opportunity to bring together a range of actors across the federal executive, as appropriate, to promote the model and enhance the identification of risks. CGU could support public entities with the use of the information obtained through analytical tools (see next section). This would help to further strengthen the SIPEF and allow the CGU, as the central body of this system, to deploy integrity risk management at the organisational level across the federal executive.

Strengthen the organisational support for integrity risk management and empower public managers

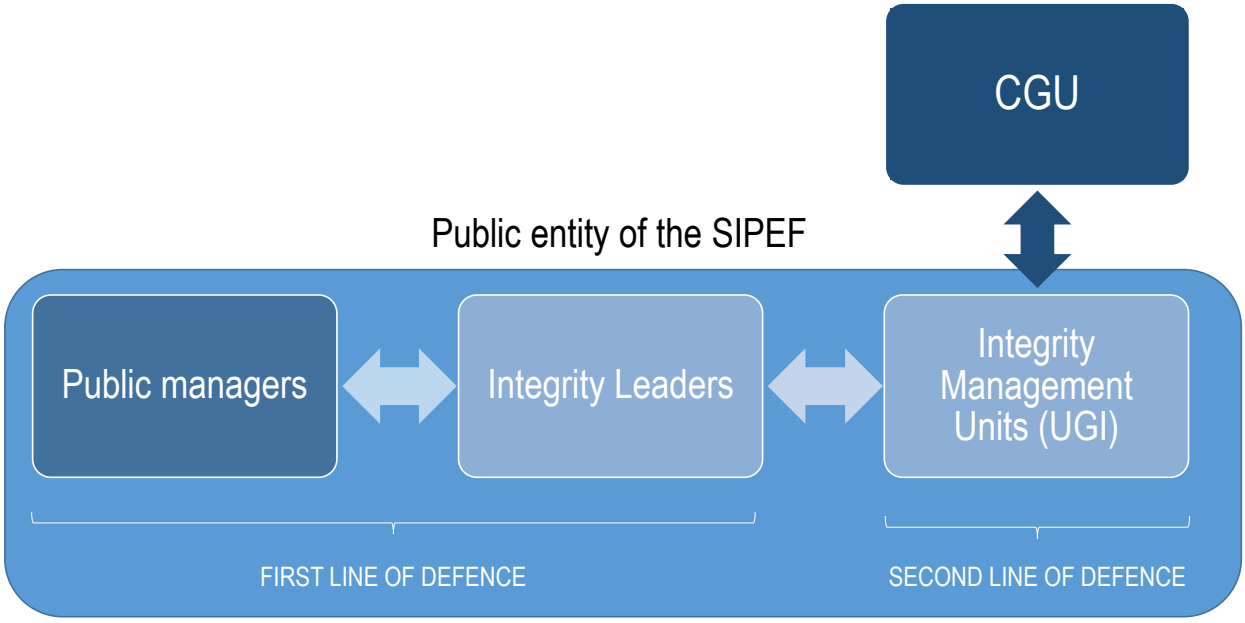
Beyond demystifying and making integrity risk management simpler and applying data analytics to support public managers, it is essential to continue developing capacities for integrity risk management across the federal executive. This includes ensuring organisational support, regular staff training, sharing of best practices, providing ad-hoc guidance etc. and covers areas such as concepts, generic integrity risks, risk assessment methodologies as well as data and IT literacy.

To reach out across the federal executive, the Integrity Management Units (UGI) play a major role in the Public Integrity System of the Federal Executive Branch (SIPEF). The UGI are responsible for providing training and assisting the areas responsible for carrying out integrity risk management, including guidance on the use of data analytics (OECD, 2021[7]). Concretely, Decree 10756/2021, which establishes the SIPEF, lays out that the UGI shall co-ordinate the management of risks to integrity. They are further responsible for steering the development of an institutional Integrity Plan, which must be based on an integrity risk analysis (CGU, 2018[9]; CGU, 2018[34]). This responsibility is key as the quality of the Integrity Plans and the proposed preventive measures depend heavily on the quality of the integrity risk assessments in the first place.

Therefore, given the pivotal role of integrity risk management for ensuring the relevance, efficiency and effectiveness of the integrity measures implemented in federal public entities, the CGU should prioritise capacity development of UGI staff in this area. The UGI, in turn, can then build on their role in the second line of assurance to reach out to public managers, providing them with guidance and support. As such, the OECD report on the SIPEF already emphasised that the UGI, in particular, could promote a better understanding of the relevance of integrity risk management amongst public managers (OECD, 2021[7]). The UGI should be able to clearly communicate about the rationale of integrity risk management and contribute to demystify the concept and to reduce fears and misunderstandings related to them. In addition, the UGI should also provide guidance and support to public managers. To do so and with help from CGU's General Co-ordination unit for Public Integrity (*Coordenação-Geral de Integridade Pública*), the UGI need to develop skills in carrying out integrity risk assessments and in providing support to public managers if needed.

To promote a culture of integrity risk management at organisational levels, however, such measures are necessary but probably not enough. To achieve cultural change, in addition to directly intervening on organisational routines, policies and procedures and providing training, behavioural insights suggest the value of influencing specific individuals in those organisations to affect organisation-wide changes (OECD, 2020[35]). In the OECD report on integrity leadership in Brazil, the role of leader as examples and integrity managers for the promotion of organisational cultures of integrity is highlighted (OECD, forthcoming[36]). The same applies of course to integrity risk management. Therefore, the UGI could start identifying a set of public managers within their entity that already are or show the potential of becoming such leaders and could become the link to other public managers, a source of knowledge and information and, not at least, a role model to follow (Figure 2.3).

Figure 2.3. The roles of CGU, the UGI and integrity leaders in promoting integrity risk management cultures in the Brazilian federal executive



Finally, the CGU is not merely providing inputs and developing capacities within the SIPEF. Integrity risk management also provides a unique opportunity for the CGU to receive quantitative and qualitative information on integrity risks collected at entity level, but also to receive feedback and collect good practices. This information about integrity risks and integrity measures can be analysed in a centralised and comparative manner by CGU's General Co-ordination unit for Public Integrity to draw conclusions about emerging and changing integrity risks, for example, or about what works and why in the prevention of these risks. For analytical purposes, this information coming from public entities of the SIPEF can be aggregated at federal level or in a way to represent specific sectors, regions or processes such as procurement or human resource management, for instance.

References

Ball, D. and J. Watt (2013), "Further Thoughts on the Utility of Risk Matrices", *Risk Analysis*, Vol. 33/11, pp. 2068-2078, https://doi.org/10.1111/risa.12057. [18]

Bemquerer Costa, M. and P. Leitão Bastos (2020), "Alice, Monica, Adele, Sofia, Carina e Ágata: o uso da inteligência artificial pelo Tribunal de Contas da União", *Controle Externo: Revista do Tribunal de Contas do Estado de Goiás*, Vol. 2/3, pp. 11-34. [30]

CGU (2018), *Guia Prático das Unidades de Gestão de Integridade*, Controladoria-Geral da União (CGU), Brasilia, https://www.gov.br/cgu/pt-br/centrais-de-conteudo/publicacoes/integridade/arquivos/unidades-de-gestao.pdf (accessed on 17 August 2021). [34]

CGU (2018), *Guia Prático de Gestão de Riscos para a Integridade: Orientações para a Administração Pública Federal direta, autárquica e fundacional*, Controladoria Geral da União (CGU), Brasilia, https://www.gov.br/cgu/pt-br/centrais-de-conteudo/publicacoes/integridade/arquivos/manual-gestao-de-riscos.pdf (accessed on 4 August 2021). [8]

CGU (2018), *Guia Prático de Implementação de Programa de Integridade Pública*, Controladoria-Geral da União (CGU), Brasilia, https://www.gov.br/cgu/pt-br/centrais-de-conteudo/publicacoes/integridade/arquivos/integridade-2018.pdf (accessed on 17 August 2021). [9]

Falk, A. and M. Kosfeld (2006), "The Hidden Costs of Control", *American Economic Review*, Vol. 96/5, pp. 1611-1630. [20]

Hallsworth, M. et al. (2018), *Behavioural Government: Using behavioural science to improve how governments make decisions*, Behavioural Insights Team, London, https://www.bi.team/wp-content/uploads/2018/08/BIT-Behavioural-Government-Report-2018.pdf (accessed on 20 January 2022). [25]

Kahneman, D. (2013), *Thinking, fast and slow*, Farrar, Straus and Giroux. [24]

Kahneman, D. and A. Tversky (1982), "On the study of statistical intuitions", *Cognition*, Vol. 11/2, pp. 123-141, https://doi.org/10.1016/0010-0277(82)90022-1. [14]

Kahneman, D. and A. Tversky (1979), "Prospect theory: An analysis of decision under risk", *Econometrica*, Vol. 47/2, pp. 263-292, https://doi.org/10.2307/1914185. [19]

Kahneman, D. and A. Tversky (1972), "Subjective probability: A judgment of representativeness", *Cognitive Psychology*, Vol. 3/3, pp. 430-454, https://doi.org/10.1016/0010-0285(72)90016-3. [15]

Loewenstein, G. et al. (2001), "Risk as feelings.", *Psychological Bulletin*, Vol. 127/2, pp. 267-286, https://doi.org/10.1037/0033-2909.127.2.267. [17]

OECD (2021), *Countering Public Grant Fraud in Spain: Machine Learning for Assessing Risks and Targeting Control Activities*, OECD Public Governance Reviews, OECD Publishing, Paris, https://doi.org/10.1787/0ea22484-en. [27]

OECD (2021), *Preventive and Concomitant Control at Colombia's Supreme Audit Institution: New Strategies for Modern Challenges*, OECD Public Governance Reviews, OECD Publishing, Paris, https://doi.org/10.1787/a2bdadf3-en. [28]

OECD (2021), *Progress report on the implementation of the Mexican Superior Audit of the Federation's mandate: Increasing impact and contributing to good governance*, OECD, Paris, https://www.oecd.org/governance/ethics/progress-report-on-the-implementation-of%20the-Mexican-Superior-Audit-of-the-Federation-s-mandate.pdf (accessed on 27 January 2022). [29]

OECD (2021), *Strengthening Public Integrity in Brazil: Mainstreaming Integrity Policies in the Federal Executive Branch*, OECD Public Governance Reviews, OECD Publishing, Paris, https://doi.org/10.1787/a8cbb8fa-en. [7]

OECD (2020), *Behavioural Insights and Organisations: Fostering Safety Culture*, OECD Publishing, Paris, https://doi.org/10.1787/e6ef217d-en. [35]

OECD (2020), *OECD Public Integrity Handbook*, OECD Publishing, Paris, https://doi.org/10.1787/ac8ed8e8-en. [1]

OECD (2019), *Analytics for Integrity: Data-driven Approaches for Enhancing Corruption and Fraud Assessments*, OECD, Paris, http://www.oecd.org/gov/ethics/analytics-for-integrity.pdf. [26]

OECD (2019), *La Integridad Pública en América Latina y el Caribe 2018-2019: De Gobiernos reactivos a Estados proactivos*, OECD, Paris, https://www.oecd.org/gov/ethics/integridad-publica-america-latina-caribe-2018-2019.pdf. [4]

OECD (2018), *Behavioural Insights for Public Integrity: Harnessing the Human Factor to Counter Corruption*, OECD Public Governance Reviews, OECD Publishing, Paris, https://doi.org/10.1787/9789264297067-en. [21]

OECD (2018), *National Risk Assessments: A Cross Country Perspective*, OECD Publishing, Paris, https://doi.org/10.1787/9789264287532-en. [3]

OECD (2017), *Recommendation of the Council on Public Integrity*, OECD/LEGAL/0435, OECD, Paris, http://www.oecd.org/gov/ethics/Recommendation-Public-Integrity.pdf. [2]

OECD (2012), *OECD Integrity Review of Brazil: Managing Risks for a Cleaner Public Service*, OECD Public Governance Reviews, OECD Publishing, Paris, https://doi.org/10.1787/9789264119321-en. [6]

OECD (forthcoming), *Behavioural Insights for Public Integrity: Strengthening integrity leadership in Brazil's federal executive branch*, OECD Publishing, Paris. [36]

OECD (forthcoming), *OECD Integrity Review of Brazil*, OECD Publishing, Paris. [5]

OECD (forthcoming), *Open Government Review of Brazil*, OECD Publishing, Paris. [32]

Ortega Nieto, D. et al. (2021), *Ethics and Corruption in the Federal Public Service: Civil Servants' Perspectives (English)*, World Bank Group, Washington D.C., http://documents.worldbank.org/curated/en/559381639027580056/Ethics-and-Corruption-in-the-Federal-Public-Service-Civil-Servants-Perspectives (accessed on 10 January 2022). [11]

Paiva, E. and F. Pereira (2021), "Extraction and enrichment of features to improve complaint text classification performance", *Anais do Encontro Nacional de Inteligência Artificial e Computacional (ENIAC)*, pp. 338-349, https://doi.org/10.5753/ENIAC.2021.18265. [33]

Schulze, G. and B. Frank (2003), "Deterrence Versus Intrinsic Motivation: Experimental Evidence on the Determinants of Corruptibility", *Economics of Governance*, Vol. 4/2, pp. 143-160, https://doi.org/10.1007/s101010200059. [22]

Slovic, P. (1999), "Trust, Emotion, Sex, Politics, and Science: Surveying the Risk-Assessment Battlefield", *Risk Analysis*, Vol. 19/4, pp. 689-701, https://doi.org/10.1111/J.1539-6924.1999.TB00439.X. [12]

Sunstein, C. and R. Hastie (2015), *Wiser: Getting Beyond Groupthink to Make Groups Smarter*, Harvard Business Review Press, Cambridge. [23]

Sunstein, C. and R. Hastie (2014), *Making Dumb Groups Smarter*, Harvard Business Review, https://hbr.org/2014/12/making-dumb-groups-smarter (accessed on 20 January 2022). [13]

TCU (2021), *Relatório anual de atividades do TCU : 2020*, Secretaria-Geral da Presidência (Segepres), Brasilia, https://portal.tcu.gov.br/data/files/99/64/46/8E/7298871003178887E18818A8/relatorio_anual_atividades_TCU_2020.pdf (accessed on 10 January 2022). [31]

TCU (2014), *Survey of Risk Management in Public Governance, Gestão De Riscos Levantamento De Governança*, Tribunal de Contas da União (TCU), Brasilia, http://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A8182A24E08D405014E0D42E95B3708 (accessed on 4 August 2021). [10]

Tversky, A. and D. Kahneman (2007), "Judgment under Uncertainty: Heuristics and Biases", *Science*, Vol. 185/4157, pp. 1124-1131. [16]

OECD Public Governance Reviews

Modernising Integrity Risk Assessments in Brazil

TOWARDS A BEHAVIOURAL-SENSITIVE AND DATA-DRIVEN APPROACH

The OECD Recommendation on Public Integrity puts risk management at the heart of any strategy or approach to ensure and promote public integrity. This report reviews the current integrity risk assessment methodology in the Brazilian federal executive branch through the lens of behavioural insights and the use of data. After presenting the methodology and analysing the challenges related to its implementation, the report provides three concrete avenues for strengthening and modernising the current approach: acknowledging and addressing cognitive and social barriers, leveraging ongoing efforts to improve the use of data and analytics for preventive purposes, and strengthening the organisational support to integrity risk management to promote a risk management culture in public entities of the federal executive.

PDF ISBN 978-92-64-57600-1