# Countering Fraud in Social Benefit Programmes

## TAKING STOCK OF CURRENT MEASURES AND FUTURE DIRECTIONS

OECD

# Countering Fraud in Social Benefit Programmes

## TAKING STOCK OF CURRENT MEASURES AND FUTURE DIRECTIONS

**Please cite this publication as:**
OECD (2020), *Countering Fraud in Social Benefit Programmes: Taking Stock of Current Measures and Future Directions*, OECD Publishing, Paris, *https://doi.org/10.1787/71df2657-en*.

ISBN 978-92-64-82786-8 (pdf)

**Photo credits:** Cover © bsd/Shutterstock.

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

# Foreword

Through social benefit programmes (SBP), governments protect individuals and families from economic and social risks, and help them lead a fulfilling life. The safety net that SBPs provide is crucial for ensuring societal well-being and a sustainable economy. For many, these programmes are a vital lifeline. Delivering SBPs means supporting businesses, households and individuals as they navigate dynamic labour markets, economic crises and changes in personal circumstances.

With social welfare expenditure representing 20 to 30 per cent of overall government spending in many OECD countries, it is essential that governments deliver SBPs effectively and efficiently. To this end, countering fraud in SBPs is critical for service delivery. Fraudulent schemes carried out by individual beneficiaries or private providers compromise the integrity of vital programmes and deprive people of essential services and social assistance. Although there are no reliable figures for global fraud levels, country-level data suggest that a significant amount of funds are lost as a result of fraud in SBPs. In the United Kingdom, for example, an estimated GBP 1.2 billion was lost from fraudulent overpayments of benefits in 2018/19. Although some of this money was later reclaimed, the amount of funds lost to fraud continues to increase each year.

Failing to counter fraud in SBPs can negatively affect public trust and undermine confidence in the government's ability to manage and deliver benefits. Trust plays a crucial role in the effectiveness of government: high trust is associated with co-operative behaviour, and low trust with resistance. A lack of public trust can undermine a government's legitimacy and jeopardise the success of public policies, programmes and regulations that rely on the co-operation of citizens. Ensuring the effectiveness and accountability of SBPs is more vital than ever in light of the increased demand placed on these programmes during the COVID-19 crisis. As many governments expand SBPs in areas such as health and income support, it is essential that they are equipped to prevent and detect fraud in an increasingly complex environment.

Mitigating risks of fraud in SBPs can help governments preserve trust while providing effective service delivery. Recognising the need to assess current approaches and provide policy makers and practitioners with insights on strengthening their anti-fraud measures, this report takes stock of what governments are doing to counter fraud in SBPs, and how they can improve. In line with the *OECD Recommendation of the Council on Public Integrity*, it focuses on preventive and detective measures, while highlighting the need to invest in the former to reduce the likelihood of fraud risks materialising at a later stage. The report explores how different actors involved in the management of SBPs can play a role in fraud prevention and detection, and how data-driven approaches are enhancing anti-fraud measures. The report also considers how governments can enhance evaluation of anti-fraud measures to help improve them. Finally, taking stock of the current state of play, it considers areas for deeper consideration and research.

This report was approved by the OECD Working Party of Senior Public Integrity Officials (SPIO) on 22nd June 2020 and declassified by the Public Governance Committee on 14th July 2020.

# Table of contents

## FIGURES

# Acknowledgements

This report was prepared by the Public Sector Integrity Division of the Directorate for Public Governance, under the direction of Julio Bacio Terracino. The report was led by Gavin Ugale and drafted by Dr Michael Nest and Lisa Kilduff. The report received contributions from the Working Party of Senior Public Integrity Officials. Jacob Arturo Rivera Perez contributed to the section on data-driven approaches to detecting fraud. Adem Kocaman provided essential editorial support.

# Executive summary

Fraud in social benefit programmes (SBP) diverts taxpayers' money away from essential services and reduces benefits for well-meaning recipients. When individual beneficiaries or private providers defraud SBPs, they jeopardise the integrity of these programmes and, in some cases, prevent governments from delivering adequate services and products. When fraud schemes are uncovered, the public's trust in government is put into question.

Through SBPs, governments provide support to families, individuals and businesses in areas such as health, employment benefits, and pensions. To ensure that governments continue to improve societal well-being and provide a safety net for those who need it, effective anti-fraud measures should be in place. Recognising the need to develop a broader understanding of this issue and the current approaches that governments are taking to counter fraud in SBPs, this report takes stock of what is currently being done and identifies areas for future research and collaboration. The report builds on the OECD's work on public sector integrity, and seeks to support policy makers and practitioners in maintaining the accountability of SBPs by highlighting good practices and areas for improvement.

## Developing effective prevention measures

This report emphasises preventive measures, including control activities, as cornerstones of governments' efforts to counter fraud in SBPs. It demonstrates how overarching strategies, when communicated to the public, can help organisations lay out their strategic vision for tackling fraud. Such strategies clearly define how an organisation envisions addressing fraud and error, and provide a roadmap for staff to counter fraud in high-risk areas. For instance, a risk-based approach would lead governments to target preventive controls at the claimant registration phase, where SBPs are most vulnerable. By focusing on preventive measures at this stage, such as simplifying processes for declaring additional income and re-registering for benefits, public organisations can minimise fraud risks at the entry point of SBPs and therefore at later stages. Ensuring that these measures are proportional allows public organisations to deliver SBPs efficiently, reducing the burden on beneficiaries where possible while countering fraud.

Alongside developing a strategy and conditions for early detection, fostering a better understanding of what motivates individuals to commit fraud helps public organisations design communication campaigns in a nuanced way, and potentially changes their approach to fraud deterrence. Governments tend to rely on punishment-oriented messaging that communicates the penalties for committing fraud. While necessary, such approaches are not entirely effective in deterring fraud. By testing and adapting fraud deterrence messaging, public organisations can ensure that control activities and public campaigns are responding to the reality of how and why individuals commit fraud.

## Improving detection tools

Technology has revolutionised the way that governments access and use data to meet policy objectives and deliver services. When it comes to SBPs, data-driven approaches have transformed how public organisations manage programmes, including preventing and detecting fraud. Through investment in intelligence capabilities and the application of data analytics techniques, data is increasingly used as a strategic resource in anti-fraud initiatives. While public organisations face challenges in leveraging data, there are opportunities to strengthen fraud prevention and detection in SBPs. In line with data protection regulations, public organisations can adopt explicit strategies to increase access to data and to allow data sharing across relevant bodies. By establishing dedicated units with the necessary skills to apply data analytics techniques, governments can ensure that data are used effectively to strengthen anti-fraud measures while promoting efficiency in service delivery.

Fraud detection can be improved by gauging how different actors play a role. Internal and external audit bodies contribute to fraud detection, and there are opportunities for public organisations to make better use of audit findings to refine their anti-fraud measures. For example, internal audit functions can identify control weaknesses that may suggest fraudulent activity or abuse, while supreme audit institutions (SAI) can provide a broader view of how effective anti-fraud measures in SBPs are. By undertaking subject-specific studies, SAIs can assess fraud and error prevention measures within public organisations, and may draw attention to systemic deficiencies in anti-fraud practices.

In SBPs, the public provides valuable information regarding suspected or potential fraud, and governments should ensure that appropriate mechanisms are in place to facilitate reporting. By making sure that hotlines and online portals are available to the public, with the option of reporting anonymously, public organisations can obtain information on potential fraud that they may not otherwise have access to. Furthermore, governments can encourage reporting by communicating the negative impact of fraud in SBPs.

## Enhancing evaluation to foster continuous improvement

Evaluation activities are crucial for improving fraud prevention and detection. If measures are ineffective, evaluations help determine alternatives and inform resource allocation. To ensure that evaluations are accurate, public organisations need to measure fraud in SBPs, which poses a number of challenges. The hidden nature of fraud and unreliable data render this process difficult. Acknowledging the variation in measurement methods used by governments and the challenges that measurement poses, public organisations can nevertheless seek to evaluate the effectiveness of their anti-fraud measures and the scale of fraud in SBPs.

As data become more readily available, there are increasing opportunities to measure fraud levels in SBPs. Establishing a baseline allows public organisations to monitor changes in the rate of fraud based on changes in the control environment, which is a critical feedback loop for managerial decision making. Once a baseline is established, the data can be used to determine the impact of control activities and whether the nature of fraud in SBPs has changed. Regularly evaluating control activities helps direct resources towards those that are cost-effective. Through analysis of evaluation results and by monitoring baselines of fraud, public organisations can produce evidence-based fraud reduction targets to support continuous improvement of fraud prevention measures.

Looking ahead, the report concludes by outlining areas that would benefit from further analysis to improve the knowledge base of the most effective anti-fraud measures. These include, but are not limited to, considering how behavioural insights can be applied to fraud prevention in SBPs, the use of data analytics and innovative methods for detecting fraud, and looking in greater depth at the link between prevention, audit and investigations.

# 1 The case for the prevention of external fraud

## 1.1. What is the issue?

Social welfare expenditure represents 20 to 30 per cent of overall government spending in many OECD countries (OECD, 2019[1]). Fraud in social benefit programmes (SBP) diverts funds away from beneficiaries and negatively affects vital services. Calculating the cost of SBP fraud is a difficult task, but country-level data suggest the amounts can be significant. In 2014, the French government detected SBP-related fraud worth an estimated EUR 425 million (French Government, 2015[2]), and in 2015, the United States Medicare Fraud Control Units recovered EUR 647 million in defrauded amounts from private providers (HHS Office of Inspector General, 2016[3]).

For the purpose of this paper, the term "social benefit programmes" refers to all government programmes that make available some kind of entitlement, whether it be a service, product or financial allowance to a beneficiary. Such programmes include tax credits and subsidies for children, unemployment benefits, subsidised or free housing, food cards (stamps), pensions, and subsidies or rebates for medical goods and services. Some SBPs involve direct transfers of money to recipients, such as pensions, unemployment benefits or disability pensions, or transfers of goods, such as housing and medical equipment. In other cases, SBPs subsidise companies and organisations that provide goods and services to beneficiaries at lower costs.

Fraud in SBPs causes more than financial losses. Fraudulent schemes can deprive people of adequate care, services and products. This can have particularly grave consequences in different sectors, such as health and social security. For instance, in Sweden, a so-called "personal assistance" scam against the Social Insurance Agency left people living with disabilities without care, while a company employed fictitious caretakers and defrauded the Swedish government by billing for work that was never performed (Radio Sweden, 2014[4]) (Allum and Gilmour, 2019[5])[1]. Furthermore, fraud in SBPs can compromise citizens' trust in government. Government integrity, defined as perceptions of the extent of both high-level corruption and low-level corruption, are the first and second most important determinants of trust in government and the civil service, respectively. Integrity is a more important determinant than many other factors, such as government reliability, responsiveness, and openness (Murtin et al., 2018[6]). While corruption is not the focus of this report, these findings are instructive. Combating fraud in SBPs is likely to help governments preserve trust while providing more effective service delivery and minimising financial losses. A lack of public integrity, even if only perceived, undermines a government's legitimacy and citizens' trust and at worst, their trust in the system overall.

The economic downturn in the wake of the COVID-19 crisis brings this obligation to the fore, as governments bolster SBPs as part of economic stimulus packages. For example, the European Commission has proposed a EUR 750 billion recovery instrument, Next Generation EU, which will prioritise the actions needed to ensure Member States' recovery in the aftermath of the crisis, and help workers keep their incomes and businesses to stay afloat. In Australia, the government announced a AUD 130

billion JobKeeper Payment scheme to help keep people in jobs in anticipation of the significant economic impact of the crisis. This is not the case everywhere. Many SBPs have experienced a drastic rise in caseloads because of the COVID-19 crisis, yet many are without an adequate increase in dedicated resources. The circumstances related to COVID-19 exacerbate existing risks, and create new challenges with implications for accountability and integrity measures.

Ensuring the integrity and accountability of SBPs is critical, in times of crisis or not. The remaining sections in this chapter provide an overview of external fraud in SBPs. The first section recognises the synergies between measures to prevent fraud and those to detect, while emphasising the additional value of the former. The chapter then addresses fundamental issues of definition, including that of "external fraud" for the purpose of this report. Finally, the chapter ends with a section that notes several critical "conditions" for fraud prevention that deserve a brief mention. This chapter sets the stage for the rest of the report, which explores governments' initiatives and tools to prevent and detect external fraud in SBPs. The report draws inspiration from the *OECD Recommendation of the Council on Public Integrity* and related international standards, as well as insights from OECD member and partner countries. The target audience of the report is policy makers and practitioners, e.g. programme managers, auditors, risk managers and anti-fraud professionals.

## 1.2. Preventive measures can result in higher returns on investment than sanctions

Governments are making progress in countering fraud in SBPs in an era of constantly evolving risks and tactics by designing tools and techniques to leverage data in their prevention efforts. To make sure that progress is sustainable, governments can strengthen their approaches further by addressing common challenges, which include:

- over-reliance on prosecution mechanisms and 'pay and chase' models that are costly and inefficient
- inaccurate or incomplete measurement of fraud
- limited risk-based approaches and evaluation of control activities
- inadequate research on behavioural aspects of fraud and what motivates perpetrators, and therefore on effective deterrence strategies
- lack of strategic thinking behind the use of data and application of data analytics tools in SBPs.

At times, public organisations rely on detection mechanisms rather than preventive controls. Both are vital, and prevention and detection mechanisms often inform each other. For example, the results of investigations or data mining may lead to changes in control activities. However, some research suggests that preventive controls yield greater cost-benefits compared to investigations and prosecutions following detection. For instance, a cost-benefit assessment of strategies for countering fraud conducted by the UK National Audit Office estimated that for every GBP 1 spent, sanctions and penalties saved GBP 1.60, whereas preventive controls saved GBP 11.45 (National Audit Office, 2015[7]).

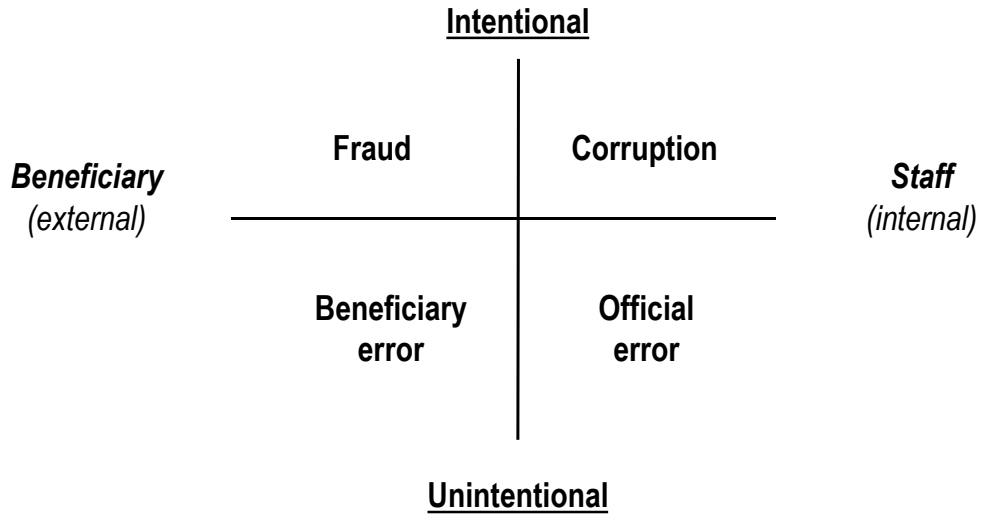
When governments rely on "pay and chase" models, they disburse entitlements and focus their anti-fraud strategies on investigations, prosecution and recovery (i.e. the "chase"). Given the nature of SBPs and the fact that they are vital for societal wellbeing, cases of fraud in SBPs draw considerable media and public attention. This visibility puts pressure on governments to produce results, usually in the form of investigations and prosecutions. While these are essential facets of an effective anti-fraud approach, they alone do not address the root causes of external fraud in SBPs or vulnerabilities in the control environment that allow fraud to occur in the first place. Instead, public organisations responsible for SBPs can adopt more cost-effective approaches that include comprehensive prevention and detection control activities to mitigate fraud risks.

## 1.3. What is "external fraud"?

Legal definitions of fraud can vary widely by country. In France, for example, the Social Security Code does not precisely define the elements of fraud, although it does refer to "abuse." By contrast, the French Labour Code defines working illegally as fraud, which has implications for unemployment benefits. Canadian legislation divides fraud into two categories: "intentional fraud" and "unintentional fraud." Unintentional fraud occurs when a recipient supplies incorrect information without the intention to deceive and obtain additional benefits (National Audit Office, 2006[8]). In Sweden, the government assumes its officials have a responsibility to ensure recipient data is accurate, putting the onus on the state as opposed to the beneficiary. When governments overpay recipients, even if this is because a recipient knowingly gave misleading data about income, the public organisation assumes it is partly responsible because of its ineffective controls. The organisation considers such acts to be error rather than fraud. By contrast, governments in countries such as the United Kingdom and the United States are more likely to place the onus for providing fully accurate data on the individual recipient. While legal definitions of fraud vary, common elements among them include: 1) a deliberate act or omission; 2) intending to deceive; and 3) intending to obtain benefits.

External fraud in SBPs, for the purpose of this report, is considered to be fraud perpetrated by individual beneficiaries or private providers of goods and services entitled to subsidies or rebates from an SBP. People often refer to this type of fraud colloquially as "welfare fraud" or "benefits fraud." In general, external fraud involves overpayments of money to recipients and is intentional and claimant-driven, as depicted in Figure 1.1. This report does not focus explicitly on improper payments, which includes fraud, waste, abuse and error, including both overpayments and underpayments. For the latter, beneficiaries are not necessarily setting out to cheat the system. They could have simply made an error in their application, or the organisation responsible for the SBP may have made a mistake when processing their application. However, many of the prevention and detection mechanisms for external fraud in SBPs discussed in this report are applicable to improper payments.

### Figure 1.1. Causes of payment discrepancies in social benefit programmes




Source: Adapted from (van Stolk and Tesliuc, 2010[9]).

Why is it important to consider external fraud as a distinct risk from internal fraud? The way in which public organisations deal with external fraud differs from how they approach internal fraud. For example, shaping organisational culture, setting the tone-at-the-top regarding fraud and corruption, ensuring separation of functions, managerial review of staff, and controls around recruitment are all essential for guarding against internal fraud. However, such controls are not sufficient for preventing and detecting fraud that is committed by an external actor.

## 1.4. Conditions for successful fraud prevention

For anti-fraud measures to succeed, at least three key conditions need to be in place, in line with the *OECD Recommendation of the Council on Public Integrity*: 1) strategic vision and commitment to implementing anti-fraud measures; 2) administrative capacity to undertake key fraud prevention, detection, and evaluation activities; and 3) public awareness and support for anti-fraud approaches.

Strategic vision for tackling fraud in SBPs can be communicated through anti-fraud initiatives and strategies, but not solely. Governments need to show commitment to prevention, and public organisations responsible for delivering SBPs need to develop implementation plans that provide clear and practical measures to fulfil the objectives of their anti-fraud strategies.

Ensuring that public organisations have the administrative capacity to carry out fraud prevention and detection activities, as well as implement adequate controls, is vital for countering fraud in SBPs. This is particularly pertinent given the availability of data analytics tools for fraud prevention and detection, an area that this report delves into more deeply in chapter 3. To take full advantage of data and the opportunities that new tools provide, it is essential that governments invest in skills development and resources. When implemented properly, these tools can simultaneously ease the administrative burden for public organisations and improve service delivery to beneficiaries.

Experience from OECD countries suggests that public awareness and support for anti-fraud approaches play a significant role in governments' adoption of anti-fraud strategies, as well as in the detection of fraud cases through reporting. As such, it is vital that governments design mechanisms to communicate and engage with the public around the issue of SBP fraud.

## Note

1 In 2015, in the Swedish town of Södertälje, 34 people were found guilty of defrauding Sweden's Social Insurance Agency. The scam involved a private company that had a contract to supply caretakers to assist people with severe disabilities and illnesses. The company employed fictitious caretakers and submitted falsified time report, billing the government for work never performed. The fake employees also qualified for allowances from the welfare system, including sick leave and parental leave. Overpayments totalled EUR 2.7 million but the trial, which took place over several years in three courts, costing the government EUR 6.6 million.

# 2 Fraud prevention measures in Social Benefit Programmes

## 2.1. Adopting a holistic approach to prevention

Typically, governments can prevent external fraud with a focus on (a) recipients of social security assistance and (b) private providers of goods and services, who are entitled to receive subsidies. The following focus areas for preventing external fraud are key:

- *Strengthening strategies, goals and objectives for combating fraud* – This includes public organisations incorporating anti-fraud prevention into their strategies, objectives and procedures, and making sure that they strike the right balance between prevention, detection and prosecution measures.
- *Targeting prevention measures at the registration phase* – To minimise the chance of fraudulent tactics succeeding at this high-risk phase, governments can ensure that they put in place adequate policies, controls and measures to verify identities and data submitted during the registration process.
- *Tailoring communication campaigns and messaging to improve fraud deterrence* – By integrating behavioural perspectives into their prevention approaches, public organisations can develop nuanced communication campaigns that include a range of messages to deter fraud in SBPs, for example by including soft messages and reminders, as well as outlining the penalties for committing fraud.
- *Focusing on the highest risks* – Risk management and assessments can contribute to savings and promote efficiency by targeting the application of preventive controls, as well as identifying areas that are susceptible to false claimants and fake registrations.

## 2.2. Strengthening strategies, goals and objectives for combating fraud

Fraud prevention measures in SBPs need to be supported by a strategic vision for how public organisations approach the problem, as well as objectives for preventing and detecting fraud. To ensure a harmonised, whole-of-government approach, the Centre of Government (CoG) may have in place policies and standards that require public organisations to combat fraud, while entities themselves can ensure that they incorporate fraud prevention into their strategies, objectives and procedures. A lack of clarity from the central level about how to implement and undertake fraud prevention measures can lead to a perception that fraud prevention objectives, and the activities that support them, are separate from other strategic and operational objectives. The CoG, as well as other bodies with government-wide responsibilities, can play a critical role in helping public organisations to overcome this challenge by providing unified standards, policies and guidance. Anti-fraud strategies or initiatives set expectations on how the government and individual entities will deal with fraud. In France, for example, the National Committee for the Fight against Fraud (*Le Comité national de lutte contre la fraude*, CNLF) co-ordinates measures to counter different

types of fraud across public organisations and state agencies. The CNLF devises multiannual national plans to combat fraud, with fraud in SBPs being one of its focus areas (Le portail de l'Économie, des Finances, de l'Action et des Comptes publics, 2016[10]). These national plans include guidance on implementing control measures, strengthening fraud risk management, and enhancing the use of data.

Despite the need for unified standards to guide fraud prevention and detection measures, the nature of SBPs requires public organisations to tailor their strategies or policies. For example, a programme aimed at providing subsidies for housing involves different processes to those that deal with unemployment benefits or support for children. As such, SBPs may be characterised by a range of fraud risks, requiring alternative measures or responses to mitigate them. In Korea, the government has responded to fraud in SBPs, and specifically those using false identities or making fake claims, by establishing the Welfare and Subsidy Fraud Reporting Center. The body is responsible for collecting and analysing fraud reports from public organisations responsible for SBPs. Its activities have resulted in savings for the government, as well as the recovery of funds obtained fraudulently within SBPs.

As part of their strategic orientation, a critical consideration for governments in the area of SBP delivery is the proportionality of anti-fraud measures to the likely impact of the risks materialising. Fraud prevention measures can affect a large number of claimants. As public organisations update and revise their anti-fraud strategies, they can consider the implications of their approach as well as the impact that new tools and technologies for fraud prevention and detection may have on society. Practically, this means taking into account the impact of strategies and detection mechanisms that cast a wide net on the public, and that focus heavily on prosecutions. It also means investing in the skills, methodologies and technology to distinguish between cases of fraud and error to ensure that well-meaning individuals receive the correct benefits. Box 2.1 provides examples of anti-fraud strategies and initiatives that seek to advance proportional approaches, and balance fraud prevention, detection and prosecution measures appropriately.

### Box 2.1. Striking the right balance when fighting fraud in social benefit programmes

Since 2014, Ireland's Department of Employment Affairs and Social Protection (DEASP) has been fine-tuning its approach to fraud prevention in social benefits programmes (SBP). The Department's updated Compliance and Anti-Fraud strategy for 2019-23 acknowledges that the vast majority of claimants are genuine and that there are no issues concerning their claims. As such, the department's strategy includes:

- continuing to target serious fraud through the work of the department's Special Investigations Unit and seconded Gardaí
- investing in predictive analytics technology to improve capacity to detect non-compliant cases
- undertaking control surveys of various schemes, including a new continuous surveying approach for some of the department's larger schemes
- publicising the department's hotline and encouraging members of the public to report cases of suspected fraud
- working collaboratively with other departments and entities and with cross-border and international organisations to prevent fraud and non-compliance.

Source: (Irish Government, 2019[11]).

## 2.3. Targeting prevention measures at the registration phase

In SBPs, registration is the first point of entry for potential claimants where governments seek to ensure that individuals receive the correct entitlements. However, this is a critical juncture for fraud prevention measures as fraudsters often target the registration process, using false data to create fake claims and identities. Furthermore, if governments fail to detect fake claimants at this stage, the perpetrators are able to continue defrauding SBPs indefinitely. A number of OECD countries experience these fraudulent tactics during the SBP registration process. For example, in 2019, French and Romanian authorities arrested several individuals charged with fraudulently obtaining welfare benefits. The perpetrators initially sought out women who claimed they were self-employed in scrap-metal recovery and convinced them to declare that they were pregnant to claim parental benefits. None of the women were in fact pregnant at the time, but the criminal group paid them to make fraudulent claims. Eventually, the perpetrators began creating fake identity cards and birth certificates of the women. In total, the syndicate registered 1 200 false identities, and in 2017 alone, collected EUR 1.7 million in benefits. Authorities found documents suggesting that the perpetrators ran similar schemes in other parts of France and Germany (Constant, 2019[12]).

This example highlights the importance of targeting prevention measures and controls at the claimant registration phase. This phase may be the only time that face-to-face interactions occur between officials and claimants, which provides an opportunity to detect identity theft. Once claimants are registered, the government may face more challenges to detect false identities for claimants with distinct names, birthdates, and addresses. Doing so often requires the use of techniques such as data-matching and data-mining, which can be resource-intensive and require special skills and expertise. To minimise the chance of fraudulent tactics succeeding at this phase, governments could ensure that they put in place adequate policies, controls and measures to verify identities and data submitted during the registration process.

At the policy level, effective fraud prevention relies on certain preconditions, such as legal and policy frameworks that facilitate data sharing between public organisations as well as with the private sector. Such frameworks are critical for effective and efficient checks of claimant information, and ensuring that public organisations respect privacy laws. Data-sharing agreements that support real-time checks can also help to reduce the burden of control on well-meaning individuals. In addition, technology can support anti-fraud measures during the registration phase. For instance, governments are employing biometrics (e.g. scanning fingers, hands, iris or face) to authenticate identities. This can serve as a control against repeated registration attempts, and help to address the challenges related to creating unique identifiers for claimants. For example, SAFE registration is the process used by Ireland's Department of Employment Affairs and Social Protection (DEASP) to establish and verify a person's identity. Completion of registration to SAFE Level 2 (i.e. substantial level of assurance of identity) is the minimum requirement for a Public Services card (PSC) to be issued. Since 2013, the DEASP has been using facial matching software to strengthen the identity authentication process by detecting and deterring duplicate registration attempts. The biometric processing of the photograph produces an arithmetic template which allows precise comparison of the photograph in question with others held by the Department. This biometric processing is performed by the Department and the arithmetic template produced is not shared with any other specified body nor is it stored on the PSC. The purpose of the PSC is to enable individuals to gain access to public services more efficiently. Furthermore, awareness and vigilance is critical. Workshops and briefings for officials on the possibility of identity fraud, as well as educational campaigns targeted at the public, can help to increase awareness and improve detection.

## 2.4. Tailoring communication campaigns and messaging to improve fraud deterrence

In order to develop appropriate measures and responses to fraud in SBPs, governments can benefit from understanding how people behave in different contexts and in response to certain incentives. Traditional attempts to tackle fraud in SBPs have included communication campaigns that focus heavily on penalties, and while this has benefits, it is not wholly effective as a deterrent. Recent studies have shown that messages focusing solely on penalties may provoke a negative emotional response that leads to them being poorly received or ignored by the very claimants they are intended to reach (Lloyd and Wilson, 2019[13]).

Such approaches tend to rely on the notion that individuals make rational cost-benefit analyses before committing fraud, when in reality such decision-making processes are not so straightforward. For example, studies have shown that in some cases, individuals commit fraud because they perceive the correct procedure as overly cumbersome (i.e. lengthy application forms and checks). As a result, they choose what appears to be the easier option and bypass a certain procedure, inadvertently committing fraud (Cabinet Office Behavioural Insights Team, 2015[14]).

In recent years, a number of governments have invested in applying behavioural insights in their tax administrations to increase compliance. Public organisations can draw lessons from these experiences to inform their fraud deterrence interventions in SBPs. For example, a recent study found that deterrence methods, in this case, letters using either harsh or soft language, had a positive impact on compliance when combined with other insights such as reinforcing social norms (Irish Government Economic and Evaluation Service, 2017[15]). These findings have implications for how public organisations may consider conveying anti-fraud messages in the delivery of SBPs. For example, communication campaigns can use a combination of 'harsh' and 'soft' messages, i.e. stating penalties and consequences, while reinforcing messages around social norms. This could include reminding individuals that the majority of claimants choose not to commit fraud, or combining reminders regarding changes of circumstances with messages about the potential penalties for fraud (See Box 2.2).

### Box 2.2. A nuanced communication campaign to deter fraud in employment insurance benefits

Service Canada is responsible for delivering the government's Employment Insurance (EI) programme, which provides temporary financial assistance to those who are unemployed or unable to work due to health reasons, as well as social assistance to other groups. For the EI programme, Service Canada has devised a communication campaign that utilises a mixture of harsh and soft messages to deter fraud. For example, the campaign includes a section on protecting the EI programme from fraud that reminds claimants that they also play a role in protecting the programme from fraud. Inclusive language is used, for example, 'We are all responsible for helping to detect and deter EI fraud'. Framing the issue of fraud prevention as a shared responsibility, with a focus on maintaining the integrity of the EI programme, demonstrates a useful example of positive framing to connect with the audience.

Furthermore, the campaign includes messages around error, making it clear to claimants that Service Canada is aware that mistakes may lead to unintended omissions or mistakes. It instructs the claimant to contact the organisation if this is the case. Service Canada combines these softer messages with reminders about the consequences and penalties for committing fraud.

Source: (Service Canada, 2020[16]).

By developing a deeper understanding of what motivates perpetrators and when individuals choose to engage in fraudulent behaviour, public organisations can design effective communication campaigns to deter fraud in SBPs. To achieve this, public organisations may consider testing the efficacy of different fraud prevention messages. This can be done using focus groups, in-depth interviews, and testing different messages in different geographical locations (i.e. local councils).

## 2.5. Focusing on the highest risks

Risk management consists of the policies, practices and tools that help an organisation to identify and mitigate risks, but more generally, facilitate informed decision-making to advance objectives. In the context of SBP and fraud, risk management is a critical pillar of prevention. Mature risk assessments incorporate both qualitative and quantitative methodologies. They help to identify and understand the effect and likelihood of risks, and then prioritise ways to spend resources on to address control weaknesses before fraud occurs. For instance, in France, the entity that provides welfare benefits, the French Social Security system's Family Branch (*Caisse d'allocations familiales*, or CAF) developed an analytical model to perform fraud risk assessments, the results of which are used to direct in-person visits and inspections towards high-risk claimants or areas (OECD, 2019[17]). Moreover, risk assessments can help managers to decide not only when to act, but when controls are sufficient for reducing risk relative to a pre-determined criteria (i.e. within risk tolerances). These criteria can include factors that are relevant for service delivery, such as the amount of time it takes to process a registration (i.e. the investment in controls) versus the likelihood and effect of a fraud risk occurring.

### Box 2.3. Targeting verifications and controls at high-risk claimants

In France, the Social Security system's Family Branch (*Caisse d'allocations familiales*, or CAF) and other social security institutions use data mining and predictive modelling to determine which beneficiaries may be at risk of committing fraud. Data mining was rolled out experimentally in 2011 and implemented in all regional branches of CAF in 2012. This technique targets additional verifications based on risk and permits claimants with a low risk score to submit less documentary evidence than those considered high risk. The predictive models allow CAF to identify cases with similar characteristics to those already identified as fraudulent.

Applications are double-checked internally to make sure that the information reported is consistent and matches the documentary evidence supplied. Furthermore, CAF checks the validity of administrative documents with the issuers (banks, internet and telephone access providers, utility companies, etc.). After review and verification of claimants' information, which is facilitated by automated exchange of information with the tax authority and a shared national social protection register, CAF targets additional verifications towards claimants with a high-risk score. For applications with the highest risk, this involves sending certified inspectors to the homes of claimants to conduct inspections and face-to-face interviews in order to determine the veracity of their claim.

Source: (Caisse d'allocations familiales, 2015[18]) (La Revue du Digital, 2018[19]).

To understand the impact of fraud risks on the entity's reputation, finances, and operations within SBPs, there are a number of high-risk areas that governments can focus on in addition to the registration phase, as described above. A high risk for SBPs is the non-declaration of additional income, often received in cash form by a recipient of benefits. Declaration of such additional income would likely reduce the recipient's benefits. In many cases, individuals may choose to omit this declaration because they do not want their benefits to decrease. However, there are a number of reasons a recipient may avoid declaring additional income. These include:

- The amount of additional income received is small, and the recipient deems it as insignificant.
- Guidelines or information about additional income are unclear or not readily available.
- The job or additional work they are undertaking may be temporary.
- Making a declaration or re-registering may require an in-person visit to the welfare office.

Declaring additional income can be a significant inconvenience, particularly if multiple trips to a welfare office are required. In the case of temporary work, the recipient may lose their right to the benefits entirely and they may be required to re-register multiple times. To deter individuals from engaging in SBP fraud in this area, governments can ensure that the process of declaring additional income is not burdensome for recipients. This could include the option of reporting additional income via email, phone or directly to a web-based personal account. Repeat registrants could be fast-tracked to facilitate the process of re-registering (Tunley, 2010[20]). This might involve a 'jump the queue' process, for example.

# 3 Improving detection techniques to target external fraud

## 3.1. Finding opportunities to enhance detection

Prevention measures are critical for mitigating external fraud risks in social benefit programmes (SBPs), but there will always be vulnerabilities in the control environment as motivated individuals or groups find new ways to exploit the system. Contributing to this is the changing landscape of payment systems and technological advancements in the distribution of SBP entitlements. When human intervention in terms of preventive measures and controls fail, automated detection strategies and tools can help SBPs to counter external fraud. The following actions are key to strengthening fraud detection in SBPs:

- *Investing in data analytics approaches and tools* – With the wealth of data that government agencies hold on claimants of SBPs, there are numerous opportunities for enhancing fraud detection. Investing in data analytics tools and capabilities can contribute not only to fraud detection, but can also facilitate real-time decision-making and responsiveness.
- *Using audit findings to target detection activities and promote a lessons-learned approach* – Internal and external audit bodies in the public sector can pinpoint vulnerabilities in fraud prevention measures and identify opportunities for improvement. To take full advantage of insights from audit bodies, including supreme audit institutions and internal audit functions, public organisations can develop approaches for compiling and analysing pertinent data from audit reports, and thereby build institutional knowledge and targeted detection activities.
- *Facilitating detection by making it easier for employees and the public to report fraud* – Given the number of suspected cases of reported fraud, governments can highlight the broader impact of fraud to reduce the perception that it is a victimless crime and motivate the public to report suspicions of fraud in SBPs.

## 3.2. Data-driven approaches to advance policy goals and detect fraud in SBPs

Technology has revolutionised the way that governments access, share and use data to meet policy objectives, design and deliver services, and streamline processes across the public sector. The digitalisation of government has also transformed how governments manage and oversee SBPs. Readily available and structured data on recipients and their claims provide opportunities for analysis and innovation through redesign. The redesign possibilities include using data to enhance service delivery and improve compliance, thus reducing fraud and error rates, and ensuring correct payments. Governments can also use analytical methods to turn raw SBP data, such as declared income, household size or place of residence, into valuable insights to improve service delivery.

Governments may also use data to improve oversight and how they detect and investigate fraud in SBPs. For example, in the United States, the Social Security Administration (SSA) maintains a 'Death Master File' of social security numbers of deceased persons. The United States Department of Agriculture (USDA) Office of Inspector General (OIG), which monitors the food stamp programme, can compare the social security numbers of applicants against this file to check for fraudulent information in the application. In a report released in January 2017, the USDA OIG entity found that 10% of applicants had used the social security number of a deceased person (Aussenberg, 2018[21]). See Box 3.1 for examples from other countries.

### Box 3.1. Data-driven fraud detection in the Czech Republic

A data matching initiative introduced by the government of the Czech Republic provides an example specifically pertaining to detection of fraud in SBPs. This initiative enables comparison of data from the Ministry of the Interior on deceased persons and place of residence, with data from employers, health insurance companies, medical institutions and labour institutions. This exercise allows public organisations to ascertain an individual's entitlement to a pension and therefore to detect erroneous or possibly fraudulent registrants.

Source: (Jorens, Gillis and De Potter, 2017[22]).

The ever-increasing availability of data and diverse analytical techniques create opportunities to design controls for processes where fraud risks are more likely to materialise, as well as to employ new tools to enhance detection measures. In one study, organisations using data analytics techniques to fight fraud reduced the financial impact of fraud schemes by 52%, and reduced the duration by 58% as a result of detection measures (Association of Certified Fraud Examiners, 2018[23]).

In addition to facilitating detection techniques, there are other implications for fraud detection in SBPs when using data as a strategic resource. For example, making better use of data can facilitate anticipatory governance and oversight by enabling real-time decision-making and responsiveness. SBPs by nature are traditionally inflexible due to the complexity of entitlement rules and the number of claimants they serve. With techniques such as data matching, entities responsible for SBPs can detect changes in claimants' circumstances in real time, drawing from automatically declared income changes. Using algorithms to automate controls, these red flags form a feedback loop to inform control activities in response to patterns that raise concern. Increasing analytical and intelligence capabilities to detect fraud within SBPs can also reduce burdens for claimants and render programme delivery more efficient (Box 3.2).

### Box 3.2. Using digital services and developing intelligence capabilities to detect fraud: The United Kingdom's Department for Work and Pensions

In 2018, in response to previous National Audit Office (NAO) recommendations, the Department for Work and Pensions (DWP) refreshed its strategy to manage Fraud, Error and Debt. Its new strategy (which the DWP will revise in 2022) focuses on understanding and identifying the causes of fraud and error, and then using this understanding to address the systemic causes. It has created:

- A Counter Fraud and Compliance Directorate (CFCD) to lead work on reducing fraud and error and recovering the resulting debts, and ensuring other parts of DWP understand their role in preventing fraud and error from occurring.
- A Risk and Intelligence Service (RIS), to better detect and understand error and fraud.
- New systems to use data-matching and up-front verification of claims to prevent and detect fraud and error. This includes better use of HM Revenue & Customs data on employment earnings (i.e. access to the Real Time Information feed).

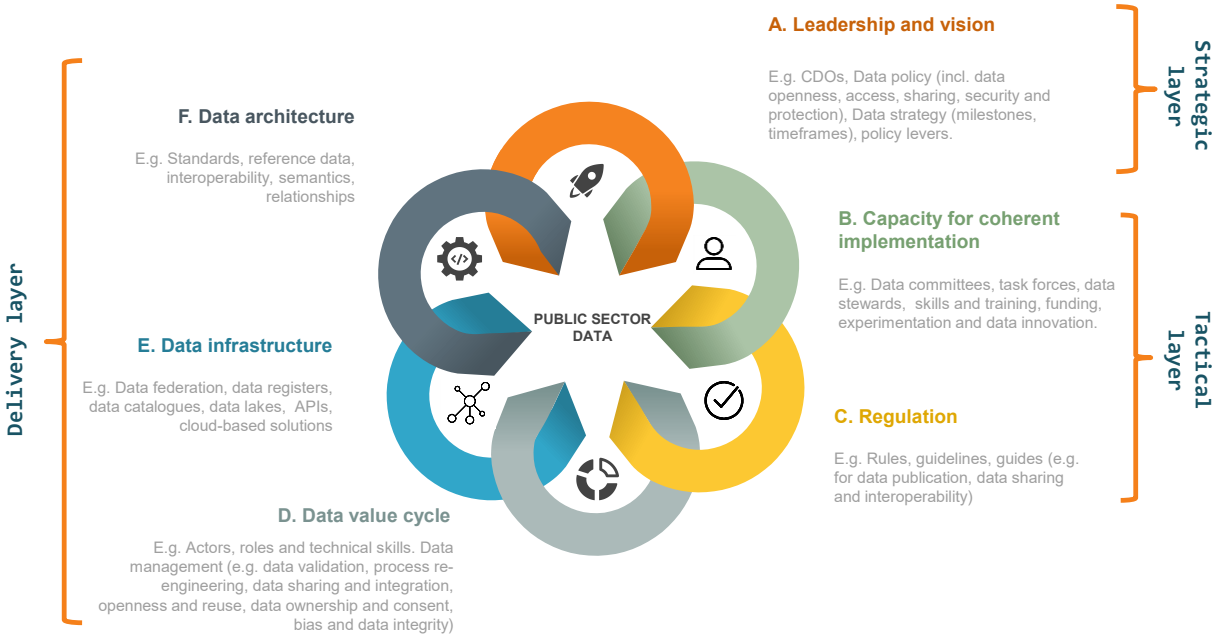
As a result of its work on determining the systemic root causes of fraud and error, the DWP found that untimely and inaccurate reporting of income and earnings remains the largest cause of fraud and error by value. In conjunction, under the Fraud Error and Debt Programme (FEDP), the DWP is transforming the way the Department prevents and detects fraud and error and how it recovers debt by delivering new digital services and replacing ageing IT systems. The DWP notes that this has produced substantial benefit and administrative savings. Its initiatives include increased use of real-time information on claimants' employment income and enhancing its analytical and intelligence capabilities.

Source: (National Audit Office, 2019[24]).

### *3.2.1. Potential challenges related to data governance and fraud detection*

While technology brings myriad opportunities for public organisations dealing with fraud, there are some challenges that governments face. As outlined in Box 3.1, data sharing among public organisations is vital when leveraging data for fraud prevention. As such, this requires a whole-of-government approach to data access and sharing, which requires strong data governance as a foundation for applying data-driven approaches to fraud detection in SBPs (see Figure 3.1). This may require addressing legacy challenges resulting from outdated legal and regulatory frameworks, or a lack of infrastructure for such technology.

## Figure 3.1. Data governance in the public sector




Source: OECD (2019), *The Path to Becoming a Data-Driven Public Sector*. Available at: https://www.oecd.org/gov/the-path-to-becoming-a-data-driven-public-sector-059814a7-en.htm.

To enhance the use of data for fraud prevention and detection in SBPs, governments can envision taking the following steps:

- Adopt an explicit policy and strategy focused on SBP optimisation through the access, sharing, use and analysis of data.
- Implement and/or revise laws, regulations or protocols allowing entities to access and share pertinent data while ensuring data protection, security and privacy. Such an approach could benefit from following an agile approach whereby stakeholders involved in the management of SBPs can better understand the legal and regulatory implications, as well as challenges associated with sharing data and providing access to data.
- Clarify institutional arrangements and responsibilities across all relevant bodies involved in the management of SBPs. This may include establishing dedicated units or teams with the necessary skills and expertise to access and process data.
- Ensure that beneficiaries of SBPs are aware of how their data are used and processed in automated SBP systems. This requires ensuring a certain level of transparency in decision-making processes related to the use of data, alongside awareness-raising initiatives to improve understanding of data-driven approaches used in SBPs.

## 3.3. Using audit findings to target detection activities and promote a lessons-learned approach

Internal and external audit bodies in the public sector play a role in preventing and detecting fraud in SBPs. Internal audit functions provide independent, objective assurance and advice to improve the efficiency and effectiveness of an organisation's operations (The Institute of Internal Auditors, 2019[25]). Auditors are expected to evaluate the potential for fraud and how an organisation manages fraud risk. This can involve

identifying fraud risk factors through their activities, with the use of analytical techniques such as data mining or data matching to highlight control weaknesses and trends that may suggest fraudulent activity or abuse in SBPs. As its mandate usually covers the processes and procedures of the organisation as a whole, internal audit is well-placed to identify common characteristics of fraud schemes or fraud risk indicators, evaluate the effectiveness of controls to prevent or detect fraud and recommend further action, including investigations. Where fraud has occurred, internal audit can provide insights on how controls failed and identify opportunities for improvement.

Although external audit bodies, or Supreme Audit Institutions (SAI), are traditionally known for their oversight of public expenditure, they are increasingly taking a broader view on reliability, effectiveness, efficiency and economy of government policies and programmes (OECD, n.d.[26]). Regarding SBPs, SAIs undertake different types of audits and activities that can contribute to fraud detection. For example, a number of SAIs have undertaken specific studies and reports to take stock of fraud and error prevention measures within public organisations, and to draw attention to sometimes systematic deficiencies in anti-fraud practices within SBPs (National Audit Office, 2015[7]) (National Audit Office, 2020[27]) (Government Accountability Office, 2018[28]).

Public organisations responsible for SBPs can leverage audit findings to improve fraud detection. Given the volume of funds that governments channel through SBPs, these programmes are typically subject to regular scrutiny by both internal and external audit functions. To take full advantage of insights from audit bodies, public organisations can develop approaches for compiling and analysing pertinent data from audit reports, and thereby build institutional knowledge and target detection activities. This includes gaining insights from the fraud risks uncovered by the government entity responsible for the SBP in question, as well as data on how effective their controls have been at preventing and detecting fraud over time. The DWP enacted the measures outlined in Box 3.2 because of audit findings produced by the NAO in previous years. As a result, the Department has invested in data analytics tools to detect fraudulent activity. Crucially, analysis of audit data, along with data from other internal and external sources (detection tools, reporting mechanisms, media reports), allows managers to prioritise controls, improve detection measures and take corrective actions where necessary (Government Accountability Office, 2015[29]).

Another example from Australia shows how audit can help uncover deficiencies in control systems and fraud prevention measures. The Auditor-General of Western Australia commissioned an audit that involved the application of data analytics techniques to four million transactions made by twelve state entities, with a total value of approximately AUD 7.5 billion (Office of the Auditor General Western Australia, 2016[30]). The audit uncovered systemic weaknesses in some of the entities control systems, revealing cases of fraud, overpayments and error. As a result, the public organisations in question reviewed their internal controls and enacted changes based on the Auditor-General's findings.

## 3.4. Facilitating detection by making it easier for employees and the public to report fraud

Information from the public can provide leads for public organisations on potential cases of fraud in SBPs. Although reports made via hotlines or online portals do not always result in the discovery of fraud, reports from the public can draw attention to certain cases that may otherwise go undetected. Strategies to promote reporting should be evidence-based to identify which reporting methods individuals consider convenient, to obtain information about the public's understanding of fraud, and the circumstances under which they would be willing to report suspected fraud. Surveys of the public are one method of obtaining such information. Other methods are focus groups with individuals who have reported fraud in the past, or interviews of officials who have received reports from the public about alleged fraud. Public organisations may also provide trainings for staff about red flags for fraud that can help them identify when to report suspicious activity.

To facilitate reporting of fraud in SBPs, public organisations should consider the following actions:

- Putting in place multiple reporting channels, e.g., email, text, phone, post, online, or via an application;
- Designing communication campaigns to inform the public on how to report suspicions of fraud, as well as raising awareness about what constitutes fraud;
- The option of anonymous reporting to encourage those who are reluctant to disclose their identity. This may be particularly relevant in cases of SBP fraud, which is likely to be detected by people close to the perpetrator;
- Timely following-up and responding to complaints to reassure individuals that their report is being treated seriously;
- Putting in place a policy within public organisations to encourage reporting by employees. Such a policy should clearly outline what reporting procedures must be followed, as well as which investigative actions will be undertaken upon receipt of a complaint.

### *3.4.1. Recognising the victims of fraud and creating incentives to report it*

In many cases, fraud in SBPs appears to have no tangible or direct impact on others; the victims are taxpayers, but such types of fraud are often considered as victimless crimes that do not directly harm others. These perceptions are strengthened by the fact that perpetrators often use false identities. However, beyond the direct financial losses for taxpayers, fraud schemes can deprive other claimants of vital services, which can be particularly serious in the case of healthcare services. Public organisations that provide SBPs should ensure that communication materials and campaigns convey the message that these are not victimless crimes, and that individuals can make a difference if they report their suspicions.

In cases where an individual directly suffers as a result of fraud, they have an incentive to report it. Using tools that collect data on clients' experiences can help detection, such as customer satisfaction surveys via email, text, post, or phone. In the private sector (such as the airline, hotel or banking industries), these surveys are often done automatically by a computer programme that contacts clients directly. Responses typically involve a rating out of 10 so the programme can add these numerical data to databases for automated analysis. Although such IT tools can be costly, they can optimise data collection and enable public organisations to reach a large number of claimants.

Following a fraud case in the United States involving faulty wheelchairs, several states have started surveying claimants to enquire about products or services provided by private companies. This information is compared to the data provided by the private providers to ensure that they had claimed the correct amount in rebates. A government entity in one state now sends surveys to claimants including photographs of wheelchairs and mobility scooters and asks them to circle the type they received. Investigators follow up on discrepancies by making on-site visits to verify the equipment (Department of Health and Human Services, 2008[31]).

# 4 Evaluation of anti-fraud measures

## 4.1. Fostering continuous improvement with evaluation

Attempting to measure fraud and determining the effectiveness and impact of fraud prevention and detection activities poses many challenges. Understanding the what, when and how of measurement is complicated by the hidden nature of fraud. Nonetheless, assessments or evaluations are vital as they offer insights into an ongoing or completed activity and inform decisions about the relevance and efficacy of fraud prevention and detection measures. This often requires the systematic collection of evidence dealing with the design, implementation and results of policies, controls and actions taken to manage fraud risks. If measures are not effective, evaluations can help determine potential alternatives for governments.

Approaches to measurement vary widely. Sample-based measurements can provide reasonable estimates for fraud and error, which can then lead to insights into what is working from a governance, oversight and control perspective. Public organisations in some countries, such as the United Kingdom, the United States and Ireland, randomly sample benefit files to detect inaccuracies. Many existing methods can lead towards underestimation or overestimation of the problem. For instance, using administrative data such as prosecutions and investigations tends to underestimate the problem, although such data can be useful inputs for measurement and evaluations. On the other hand, perception-based measurements can overestimate the prevalence of fraud and error in a system.

There are a number of ways that public organisations can measure and evaluate how effective their fraud prevention and detection measures are. These include:

- *Evaluating control activities* - Measuring the efficacy of controls allows governments to put in place results-based performance management systems to ensure that fraud prevention is part of employees' daily tasks.
- *Establishing baselines and assessing cost-effectiveness of anti-fraud measures* - Measuring changes in the rate of fraud can help determine the impact of control activities. However, this is only possible if a baseline is established and if data on fraud are routinely collected.
- *Setting annual targets for fraud prevention and publishing results* – This can enable public organisations to evaluate their prevention and detection activities while incentivising managers in their efforts to reduce fraud in SBPs.

## 4.2. Evaluating control activities

Public organisations should evaluate their anti-fraud control activities to determine what is working and where there is room for improvement. This includes testing control design effectiveness and the operational effectiveness of a control. The need for evaluation is reflected in international standards, such as Principle Five of the Fraud Risk Management Guide developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO). The guide describes how establishing measurement criteria enables monitoring and evaluation, as well as analytical comparisons of an organisation's fraud risk management activities (Committee of Sponsoring Organizations of the Treadway Commission, 2016[32]). Many public

organisations adhere to an anti-fraud policy or risk management standards that are implemented and harmonised across government. However, due to the nature of SBPs and the unique way in which responsible entities interact with the public, as well as the sheer number of beneficiaries, the approach to evaluation of anti-fraud control activities may differ.

While countries are adopting new methods and tools to tackle fraud in SBPs, there is still considerable progress to be made regarding how public organisations monitor and evaluate their fraud prevention and detection measures. Entities may face challenges measuring outcomes of their anti-fraud control activities in a reliable way. These challenges include the difficulty of measuring the extent of deterred fraud, isolating potential fraud from legitimate activity or other forms of improper payments, and determining the amount of undetected fraud (Government Accountability Office, 2015[29]). Despite these challenges, there are ways that managers can test the effectiveness of their control measures and the short-term or intermediate outcomes of these activities. For example, monitoring the activities of dedicated anti-fraud units and the number of potential or real cases of fraud they uncover when reviewing recipients' claims is a simple way of assessing their impact on fraud levels.

To assess operating effectiveness of control activities, public organisations can do a "walkthrough" of end-to-end processes with the appropriate personnel, mapping out areas at-risk to potential fraud with the corresponding control activity. Applied to claimant registration processes in SBPs, this mapping could lay out each step and specify the key controls, whether they are manual or automated, and how frequently they are applied. Most importantly, the walkthrough should detail how the operation of the control is evidenced, i.e. sign-off processes by different levels of staff, secondary review mechanisms, receipt of cross-referenced documentation. This is just one way that entities can assess control effectiveness. Other methods include examination and inspection tests, re-performance of control activities, and inquiries into control effectiveness. Many key controls are likely to be subject to existing internal or external audit reviews; this should be taken into consideration in control test planning schedules.

## 4.3. Establishing baselines and assessing cost-effectiveness of anti-fraud measures

Evaluation of anti-fraud measures can complement other assessments to understand baselines for levels of fraud and cost-effectiveness of anti-fraud measures. A baseline allows for monitoring changes in the rates of fraud based on changes in the control environment, which is a critical feedback loop for managerial decision-making. Without such baselines, it is difficult for entities to measure the efficacy of control activities. If data are available, public organisations can draw from statistical models to determine fraud rates and create baselines (OECD, 2019[17]). While a baseline for fraud levels is difficult to establish, governments can consider several approaches, including the following:

- Examining historical data for fraud to establish a fraud rate, preferably time-series data over a number of years, i.e. what percentage of claims are fraudulent, what percentage of recipients submitted a fraudulent claim.
- Undertaking comprehensive, large-scale audits or risk assessments to help establish the rate of fraud based on identifying cases of suspected fraud. If fraud is confirmed, results can then provide insights into a likely fraud rate based on programme size (e.g. number of recipients; value of detected frauds), although it may not be possible to generalise or apply findings from the results.
- Random sampling of cases where there is a specific focus on finding suspicious cases. Given proper methodological design, identified results can be generalised to entire programmes (OECD, 2019[17]).

These approaches can help governments to benchmark their progress and foster a long-term view of fraud prevention in SBPs. Examples of metrics that can inform the development of the baseline include:

- the number, percentage and value of fraudulent claims identified
- the number and percentage recipients committing fraud
- the number and percentage of private providers committing fraud
- the number, percentage and value of fraudulent transactions involving different goods and services across SBPs
- control weaknesses or fraudulent activity uncovered through inspections or audits.

Once a baseline of fraud is established and new control activities are applied, it is easier for governments to monitor if levels of fraud are affected, as well as to identify trends and higher risk areas.

Baselines can also be inputs for cost-benefit analyses. Determining whether control activities are cost-effective can also be a difficult task depending on what data are available. Estimating the return on investment (ROI) in approaches to tackling fraud is not self-evident, and particularly when data analytics models have been implemented, it may be necessary to assess the total cost of ownership of these models as well as the impact of fraud on the entity, which is difficult to determine. Assessing the cost-effectiveness of fraud prevention measures cannot be boiled down to typical, numerical ROI calculations given difficulties in determining the number of fraudulent cases prevented. Despite these limitations, entities responsible for SBPs can keep track of certain observations as part of the baseline analysis to determine if their control activities are cost-effective. For example, monitoring the number of newly detected cases over a certain period, or changes in the number of cases that were detected early compared to previous cases.

## 4.4. Setting annual targets for fraud prevention and publishing results

For public organisations that are responsible for delivering SBPs, setting annual targets for fraud reduction or prevention measures can facilitate the measurement of fraud. This is a practice observed in some OECD countries. In Canada and New Zealand, respectively, the government has developed fraud reduction-related targets for managers responsible for SBPs (OECD, 2019[17]). As well as reducing fraud levels and enabling measurement, the introduction of such targets can also have implications for performance management within public organisations (Box 4.1).

### Box 4.1. Measuring progress of fraud prevention measures: The integrated approach of the Department of Employment Affairs and Social Protection in Ireland

In line with the strategic objectives of its Compliance and Anti-fraud Strategy, the Department of Employment Affairs and Social Protection (DEASP) publishes an annual report on its fraud prevention and detection activities. These reports provide an account of how the Department has performed over the previous year in pursuing its goals of reducing incidents of fraud and non-compliance in Ireland's social welfare system. The reports present key outcomes of the Department's activities, for example, how many claims were reviewed, the estimated total savings resulting from their implemented measures, and detection rates of overpayments, among others. In addition, the Department provides details on trends in fraudulent practices within SBPs and the most common tactics employed by those committing fraud. This is followed by an overview of how the Department has adopted new methods to prevent and detect fraudulent activity, for example by strengthening its investigation unit and applying different data analytics techniques.

Following the presentation of the Department's activities, the report lays out the priority areas for the subsequent year and sets specific targets in its Annual Target Statement. This approach provides comparative data for the Department to assess its progress as well as areas for improvement. These reports have been produced annually since 2014 to support the implementation of the Compliance and Anti-fraud Strategy. As a result, the Department of Employment Affairs and Social Protection reports that it has increased detection rates of fraud in SBPs and strengthened its prevention measures.

Source: (Irish Government, 2017[33]).

# 5 Future directions to mitigate external fraud risks

This report highlights key areas for improvement to prevent and detect external fraud in SBPs. By addressing certain gaps in current prevention, detection and evaluation measures, governments can strengthen their anti-fraud approaches and ensure that they deliver SBPs efficiently. Taking action against external fraud not only leads to fewer financial losses, but also non-financial gains in terms of better service delivery and preservation of trust in government. As described in this report, governments and responsible entities can take concrete steps to prevent, detect and evaluate external fraud in SBPs.

## 5.1. An ounce of prevention is worth a pound of cure

An overarching strategy that communicates the strategic vision for tackling fraud is vital. This provides staff with a roadmap for how the entity plans to approach the issue of external fraud, differentiating it from other types of improper payments. Also, communicating the strategy to the public can help build trust and demonstrate that the organisation is committed to reducing fraud in SBPs.

The report highlights the need to ensure effective controls in the claimant registration phase of SBPs. As evidenced in many countries, this stage is particularly susceptible to fraud. By targeting preventive controls at this stage and simplifying processes for declaring additional income and re-registering for benefits, entities can minimise fraud risk and potentially prevent individuals from committing fraud at a later stage.

Linked to this is the need to understand what motivates individuals to commit fraud and to design communication and deterrence campaigns in a nuanced way. By testing and adapting fraud deterrence messaging, public organisations can ensure that control activities and public campaigns are responding to the reality of how and why individuals commit fraud. This helps governments move away from traditional, punishment-focused approaches that are costly and inefficient to fraud prevention. Last, using risk management to prioritise and target control activities can render service delivery more cost-efficient and strengthen fraud prevention efforts.

## 5.2. Enlisting technology and people for better detection

The report highlights the opportunities for public organisations that are responsible for SBPs to use data as a strategic resource. By investing in tools to facilitate fraud detection and developing intelligence capabilities, entities have a better chance of early detection when it comes to potential or actual fraud. Furthermore, data analytics tools and techniques such as data matching can facilitate real-time decision making and monitoring of fraud risks, as well as identifying red flags for fraud in data sets.

Internal and external audit bodies contribute to fraud detection, and there are opportunities for public organisations to make better use of audit findings to hone their anti-fraud measures. Internal audit functions can identify control weaknesses and trends that may suggest fraudulent activity or abuse, while supreme

audit institutions (SAI) can provide a broader view and analysis of whether anti-fraud measures in SBPs are effective. Thematic studies and reports undertaken by SAIs can draw attention to deficiencies and provide recommendations on where public organisations can make improvements.

In SBPs, the public provides valuable information regarding suspected or potential fraud, and governments should therefore ensure that there are appropriate mechanisms in place to facilitate reporting. By ensuring that hotlines and online portals are available to the public, with the option of reporting anonymously, public organisations can gain information on potential fraud that they may not otherwise have access to. Strategies to promote reporting should be evidence-based to identify which reporting methods are most effective in obtaining information from the public. Furthermore, governments can encourage reporting by communicating about the impact of fraud in SBPs. Often perceived as a victimless crime, fraud diverts funds from vital programmes and deprives beneficiaries of SBPs of services.

## 5.3. Evaluating what works

As data are becoming more readily available, there are increasing opportunities to measure fraud levels in SBPs. In line with the previous recommendations on using data as a strategic resource, public organisations can leverage data in SBPs and extract certain data points to track fraud levels and determine fraud patterns, which in turn can inform control activities. A baseline allows for monitoring changes in the rates of fraud based on changes in the control environment, which is a critical feedback loop for managerial decision-making. If data are available, public organisations can draw from statistical models to determine fraud rates and create baselines.

In addition, evaluating control activities regularly helps direct resources towards those that prove to be cost-effective. While acknowledging that there are certain challenges in measuring outcomes of anti-fraud control activities, public organisations can adapt their evaluation methods in line with their capacity and resources. By analysing the results of evaluations and monitoring baselines of fraud, public organisations can produce annual fraud reduction targets that are evidence-based and realistic. This serves to incentivise managers and employees to meet anti-fraud requirements while promoting a more comprehensive approach to designing and implementing fraud control activities.

## 5.4. Areas to explore further

This report is a stocktaking of select challenges and issues; however, external fraud in SBPs and government responses to it are complex and constantly evolving. COVID-19 and the subsequent economic turmoil exacerbated existing risks that have long affected SBPs, and created new risks and challenges as governments respond to calls for relief from individuals and businesses. The stocktaking exercise for this report highlighted several areas that would benefit from further analysis to improve the knowledge base around what prevention and detection measures are most effective. The list below is not exhaustive, and many of these issues are not exclusive to external fraud in SBPs. However, like any area, countering fraud in SBPs requires a tailored approach to account for context, including the policies and procedures for the goods or service provided.

- **Policies, strategies and guidance across government and within institutions** – The tools and skills to prevent and detect fraud are critical, but are a second priority for many governments and public organisations that lack a coherent strategy and guidance to use them well. For instance, without the legal frameworks for data sharing, investments in data matching by SBPs is of limited value. Future research and support for governments can help to further articulate the key issues and “preconditions” for effective fraud prevention and detection in SBPs, to support both Centre of Government institutions and individual institutions to prioritise actions. In addition, strategies for

striking a balance between controls and service delivery are critical, particularly in the context of economic crises and post-pandemic stimulus packages. Good practices for developing a strategic, co-ordinated response to proportionality and oversight is critical for SBPs that are operating under such circumstances.

- **Use of data and analytics** – Along the data value chain—generation, processing, sharing and use or (re)use of information for data-sharing—there are many challenges and opportunities for public organisations to improve their use of data for mitigating fraud risks in SBPs. This includes both government-wide and institutional level improvements to data strategies, skills, tools and methodologies. The OECD and others have a rich body of work on digital government and data-driven tools that could be consolidated and tailored to the SBP context to improve data-driven fraud prevention and detection.
- **Innovative methods for detecting fraud** – In addition to what are now "traditional" forms of data analytics, like data matching and data mining, public organisations are adopting and experimenting with many other innovative methods to prevent and detect external fraud that are applicable for SBPs. For instance, some private and public organisations are developing methodologies to sift through social media that reveals a lifestyle at odds with their purported entitlements, or using drones to survey areas following a disaster to inform eligibility criteria for relief funds. Fraud prevention and detection relies on multiple solutions carried out in parallel. Future research can uncover lessons learned from innovative initiatives that are cost-effective and can be added to the government's anti-fraud arsenal.
- **Baselines and cost-benefit analyses** – A major challenge facing public organisations when it comes to evaluating the effectiveness of anti-fraud measures is the creation of baselines and conducting cost-benefit analyses. Skills, knowledge, and linking control measures to impacts that are inherently hidden and therefore difficult to measure are some of the persistent challenges. Future analysis and testing of new approaches, including quantitative assessments, could help governments to bolster their capacities in this area. In SBPs, baselines and cost-benefit analysis could consider both internal and external fraud risks involving beneficiaries, contractors and other service providers.
- **The link between prevention, audit and investigations** – Public organisations often make referrals to investigative bodies and then never receive feedback about the results, or they fail to absorb the recommendations or use the work of internal and external audit bodies. This break in the communication, co-ordination between entities or uptake of recommendations results in missed opportunities. Opportunities include improvements to risk assessments, control activities and reporting mechanisms for better fraud prevention and detection. Future work could explore how governments can best develop a 'lessons learned' approach from investigations and audits, which could include good practices for compiling and analysing results of investigative and audit reports, behavioural insights to enhance the use of audit recommendations and understanding the modus operandi of perpetrators.
- **Applying behavioural insights** - Existing efforts to prevent fraud and corruption are still widely based on a rational decision-making model, an approach that stresses the importance of increasing the costs and lowering the benefits of undesired behaviour. However, in recent years there has been a shift towards thinking about corrupt or unethical behaviour with a focus on addressing apparently "irrational" decision-making. Indeed, social context and behavioural biases often influence people's abilities to act rationally and ethically. Governments could further explore the applicability of behavioural approaches in the SBP context, particularly to better understand and countervail fraud committed by those who failed to rationally consider the consequences both for them and others (OECD, 2018[34]). Governments could further explore the applicability of behavioural approaches in the SBP context, particularly to prevent fraud committed by those who failed to report income without rational consideration of the consequences.

# References


Allum, F. and S. Gilmour (eds.) (2019), *Handbook of Organised Crime and Politics*, Edward Elgar Publishing, https://www.e-elgar.com/shop/gbp/eelgar/product_flyer/generate/id/14627/. [5]

Association of Certified Fraud Examiners (2018), *Report to the Nations: 2018 Global Study on Occupational Fraud and Abuse*, https://s3-us-west-2.amazonaws.com/acfepublic/2018-report-to-the-nations.pdf. [23]

Aussenberg, R. (2018), *Errors and Fraud in the Supplemental Nutrition Assistance Program (SNAP)*, Congressional Research Service, https://digital.library.unt.edu/ark:/67531/metadc1157055/. [21]

Cabinet Office Behavioural Insights Team (2015), *Applying Behavioural Insights to Reduce Fraud, Error and Debt*, http://38r8om2xjhhl25mw24492dir.wpengine.netdna-cdn.com/wp-content/uploads/2015/07/BIT_FraudErrorDebt_accessible.pdf. [14]

Caisse d'allocations familiales (2015), *The Family Branch of the French Social Security System*, https://www.caf.fr/sites/default/files/Anglais%20Pr%C3%A9sentation%20branche%20famille_2015.pdf. [18]

Committee of Sponsoring Organizations of the Treadway Commission (2016), *Fraud Risk Management Guide*. [32]

Constant, J. (2019), *"Escroquerie à la CAF de Valenciennes : quatre personnes arrêtées en Roumanie"*, http://www.leparisien.fr/faits-divers/escroquerie-a-la-caf-de-valenciennes-quatre-personnes-arretees-en-roumanie-08-05-2019-8067894.php (accessed on 29 May 2020). [12]

Department of Health and Human Services (2008), *Medicaid Integrity Program - Georgia Comprehensive Program Integrity Review*, https://www.cms.gov/Medicare-Medicaid-Coordination/Fraud-Prevention/FraudAbuseforProfs/Downloads/GAfy08.pdf. [31]

French Government (2015), *Dossier de Presse : Comité national de lutte contre la fraude*, https://www.economie.gouv.fr/files/files/directions_services/dnlf/DOSSIER_DE_PRESSE_Comite_National_de_Lutte_contre_la_Fraude-_Mardi_23_juin_2015%281%29.pdf. [2]

Government Accountability Office (2018), *Supplemental Nutrition Assistance Program: Disseminating Information on Successful Use of Data Analytics Could Help States Manage Fraud Risks*, https://www.gao.gov/products/GAO-19-115 (accessed on 29 May 2020). [28]

Government Accountability Office (2015), *A Framework for Managing Risks in Federal Programs*, https://www.gao.gov/assets/680/671664.pdf. [29]

HHS Office of Inspector General (2016), *Medicaid Fraud Control Units Fiscal Year 2015 Annual Report*, https://oig.hhs.gov/oei/reports/oei-07-16-00050.asp (accessed on 29 May 2020). [3]

Irish Government (2019), *Compliance and Anti-fraud Strategy: 2019 to 2023*, Department for Employment Affairs and Social Protection, https://assets.gov.ie/73317/60ba11ca1f8847be82ee1d6808e16404.pdf. [11]

Irish Government (2017), *Compliance & Anti-Fraud Strategy 2014-2018: Annual Report 2016 & Annual Targets Statement 2017*, Department of Social Protection, https://www.gov.ie/pdf/?file=https://assets.gov.ie/74861/aa945625-d301-4145-b7be-40aa1a602ce4.pdf#page=null. [33]

Irish Government Economic and Evaluation Service (2017), *Applying Behavioural Science in Tax Administration - A Summary of Lessons Learned*, https://www.revenue.ie/en/corporate/documents/research/applying-behavioural-science.pdf. [15]

Jorens, Y., D. Gillis and T. De Potter (2017), *Fraud and Error in the Field of EU Social Security Coordination*, https://ec.europa.eu/social/BlobServlet?docId=18645&langId=en. [22]

La Revue du Digital (2018), *Le Data Mining aiguillonne la détection des cas de fraude à la Caf : +5% en 2017*, https://www.larevuedudigital.com/le-datamining-aiguillonne-la-detection-des-cas-de-fraudes-a-la-caf/ (accessed on 29 May 2020). [19]

Le portail de l'Économie, des Finances, de l'Action et des Comptes publics (2016), *"Le Comité national de Lutte contre la Fraude adopte son plan triennal"*, https://www.economie.gouv.fr/le-comite-national-de-lutte-contre-la-fraude-2016-adopte-son-plan-triennal (accessed on 29 May 2020). [10]

Lloyd, M. and P. Wilson (2019), *Fraud and Error Deterrence/Prevention Message Testing*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/784321/fraud-and-error-deterrence-prevention-message-testing.pdf. [13]

Murtin, F. et al. (2018), "Trust and its determinants: Evidence from the Trustlab experiment", *OECD Statistics Working Papers*, No. 2018/2, OECD Publishing, Paris, https://dx.doi.org/10.1787/869ef2ec-en. [6]

National Audit Office (2020), *Universal Credit Advances Fraud*, https://www.nao.org.uk/wp-content/uploads/2020/03/Universal-Credit-advances-fraud.pdf. [27]

National Audit Office (2019), *Departmental Overview 2019 - Department for Work & Pensions*, https://www.nao.org.uk/wp-content/uploads/2019/10/Overview-Department-for-work-and-pensions-2019.pdf. [24]

National Audit Office (2015), *Fraud and Error Stocktake*, https://www.nao.org.uk/wp-content/uploads/2015/07/Fraud-and-error-stocktake.pdf. [7]

National Audit Office (2006), *International Benchmark of Fraud and Error in Social Security Systems*, https://www.nao.org.uk/wp-content/uploads/2006/07/05061387.pdf. [8]

OECD (2019), *Social Expenditure Update 2019 – Public Social Spending is High in Many OECD Countries*, OECD, Paris, https://www.oecd.org/social/soc/OECD2019-Social-Expenditure-Update.pdf. [1]

OECD (2019), *The Path to Becoming a Data-Driven Public Sector*, OECD Digital Government Studies, OECD Publishing, Paris, https://dx.doi.org/10.1787/059814a7-en. [17]

OECD (2018), *Behavioural Insights for Public Integrity: Harnessing the Human Factor to Counter Corruption*, OECD Public Governance Reviews, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264297067-en. [34]

OECD (n.d.), *"External Audit – Supreme Audit Institutions"*, https://www.oecd.org/gov/external-audit-supreme-audit-institutions.htm (accessed on 29 May 2020). [26]

Office of the Auditor General Western Australia (2016), *Audit of Payroll and other Expenditure using Data Analytic Procedures*, https://audit.wa.gov.au/wp-content/uploads/2016/05/report2016_06-DataAnalytics.pdf. [30]

Radio Sweden (2014), *"Södertälje court convicts 34 people in welfare fraud case"*, https://sverigesradio.se/sida/artikel.aspx?artikel=5891564 (accessed on 29 May 2020). [4]

Service Canada (2020), *"Employment Insurance and fraud"*, https://www.canada.ca/en/employment-social-development/programs/ei/ei-list/reports/fraud-serious.html#h2.5 (accessed on 29 May 2020). [16]

The Institute of Internal Auditors (2019), *Fraud and Internal Audit*, https://na.theiia.org/about-ia/PublicDocuments/Fraud-and-Internal-Audit.pdf. [25]

Tunley, M. (2010), "Need, greed or opportunity? An examination of who commits benefit fraud and why they do it", *Security Journal*, Vol. 24/4, pp. 302-319, http://dx.doi.org/10.1057/sj.2010.5. [20]

van Stolk, C. and E. Tesliuc (2010), *Toolkit on Tackling Error, Fraud and Corruption in Social Protection Programs*, RAND Corporation, https://www.rand.org/pubs/working_papers/WR746.html. [9]

# Countering Fraud in Social Benefit Programmes

## TAKING STOCK OF CURRENT MEASURES AND FUTURE DIRECTIONS

This report takes stock of approaches taken by public organisations to counter external fraud in social benefit programmes (SBP) and suggests areas for improvement. It provides insights on preventive and detective measures, and promotes a risk-based approach to addressing fraud and error in SBPs in line with the OECD Recommendation of the Council on Public Integrity. It explores how public organisations can leverage data-driven approaches to improve fraud detection, and how strengthening evaluation activities can promote continuous improvement of anti-fraud measures.

**PDF ISBN 978-92-64-82786-8**

9 789264 827868