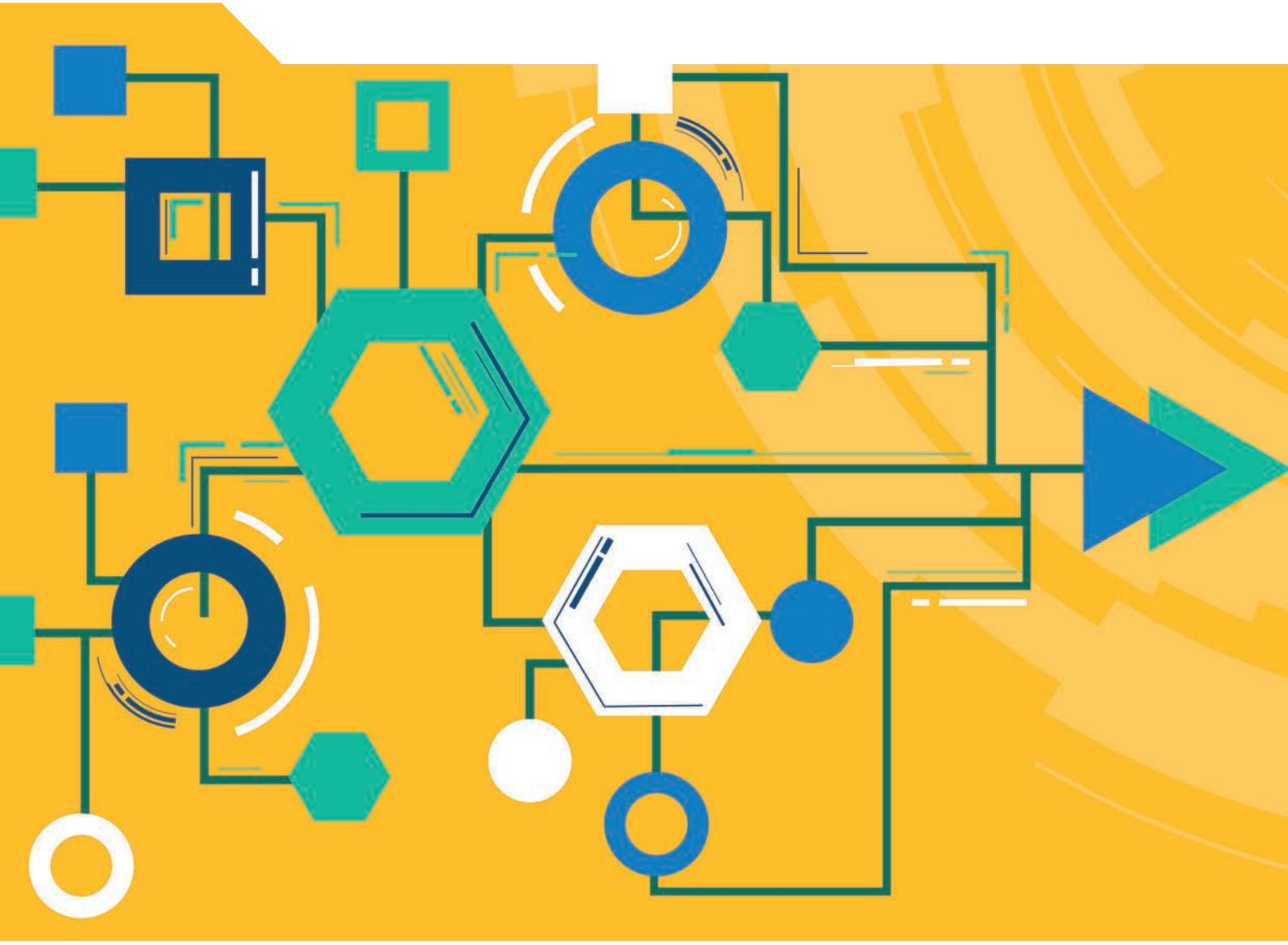
OECD Public Governance Reviews

Tackling Fraud and Corruption Risks in the Slovak Republic

A STRATEGY WITH KEY ACTIONS FOR THE EUROPEAN STRUCTURAL AND INVESTMENT FUNDS



OECD

OECD Public Governance Reviews

Tackling Fraud and Corruption Risks in the Slovak Republic

A STRATEGY WITH KEY ACTIONS FOR THE EUROPEAN STRUCTURAL AND INVESTMENT FUNDS



BETTER POLICIES FOR BETTER LIVES

This work is published under the responsibility of the Secretary-General of the OECD. The opinions expressed and arguments employed herein do not necessarily reflect the official views of OECD member countries.

This document, as well as any data and any map included herein, are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Please cite this publication as:
OECD (2019), *Tackling Fraud and Corruption Risks in the Slovak Republic: A Strategy with Key Actions for the European Structural and Investment Funds*, OECD Public Governance Reviews, OECD Publishing, Paris, *https://doi.org/10.1787/6b8da11a-en*.

ISBN 978-92-64-56816-7 (print)
ISBN 978-92-64-93625-6 (pdf)

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

Photo credits: © Cover designed by We are Flint.

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

© OECD 2019

You can copy, download or print OECD content for your own use, and you can include excerpts from OECD publications, databases and multimedia products in your own documents, presentations, blogs, websites and teaching materials, provided that suitable acknowledgement of OECD as source and copyright owner is given. All requests for public or commercial use and translation rights should be submitted to *rights@oecd.org*. Requests for permission to photocopy portions of this material for public or commercial use shall be addressed directly to the Copyright Clearance Center (CCC) at *info@copyright.com* or the Centre français d'exploitation du droit de copie (CFC) at *contact@cfcopies.com*.

Foreword

Through the European Structural and Investment (ESI) Funds, the European Union invests billions of euros in job creation and a sustainable and healthy European economy and environment. Programmes to boost employment, education, social equity, competition, and agriculture rely on a EUR 450 billion budget for the programming period of 2014-20. These investments are critical for the development and growth of economies across EU Member States.

Given the size of these financial flows, it is of paramount importance that the right mechanisms are put in place to mitigate the risks of misappropriation of funds. Fraud and corruption divert taxpayers' money away from investments intended to boost job creation and socio-economic development. Ultimately, this can poison public trust.

During the current programming period, the government of the Slovak Republic has faced threats to the integrity of the ESI funds. In response, it embraced a holistic approach, recognising the need to improve not only the detection and investigation of fraud and corruption, but also prevention through risk management and internal control.

As part of its work to help countries battle fraud and corruption, the OECD assisted the government of the Slovak Republic in modernising its risk management strategy for ESI Funds. Recognising the existing, robust normative and policy frameworks, the OECD focused on overcoming implementation challenges. The result is a plan of action that offers tailored guidance for both Managing Authorities, who play a critical role at the operational level, and centre of government bodies, who take the overall lead in this area. The strategy proposes concrete actions for refining risk assessments and mitigations, and it includes suggestions for greater precision of the risk assessment process through better use of data.

Apart from rigorous risk assessment, effectively handling fraud and corruption risks requires a robust risk management culture, so that assessments lead to better decision-making. As new risks emerge, the government will need to focus on further improving capacity and skills. The strategy presented here provides guidance on the necessary steps for doing so, along with insights on how to monitor and evaluate the entire risk management framework. Better co-ordination among managing authorities, central government, the Public Procurement Office, law enforcement and regulatory bodies can help to make further progress.

Preventing fraud and corruption in ESI Funds is a shared responsibility. The strategy outlines key actions to promote a common understanding of those responsibilities, with guidance for fulfilling them. The strategy draws from the *OECD Recommendation of the Council on Public Integrity* and related international standards, as well as insights from OECD member and partner countries. Its ultimate goal is to foster more effective, integrity-driven policies for better lives and outcomes for Slovak citizens.

Acknowledgements

This strategy was prepared by the Public Sector Integrity Division of the Directorate for Public Governance under the leadership of Janos Bertók and Julio Bacio Terracino. The strategy was drafted by Gavin Ugale, Lisa Kilduff, and Angelina Zhao. The strategy benefitted from insights provided by Angelos Binis. Editorial and administrative support was provided by Meral Gedik, Rania Haidar, Aleksandra Bogusz, and Thibaut Gigou.

The OECD expresses its gratitude to the government of the Slovak Republic for its commitment and co-operation in developing this strategy, in particular Denisa Žilláková, General Director of the Central Co-ordination Body, Office of the Deputy Prime Minister for Investments and Informatisation, Matúš Drotár, Director of the Department of Methodology and Coordination of Institutions within the Central Co-ordination Body, Office of the Deputy Prime Minister for Investments and Informatisation, and Igor Jašurek, Senior Expert within the Department of Methodology and Coordination of Institutions of the Central Co-ordination Body, Office of the Deputy Prime Minister for Investments and Informatisation. The OECD would also like to thank the Ministry of Education, Science, Research and Sport, the Ministry of Environment, the Ministry of Transport and Construction, the Ministry of Labour, Social Affairs and Family, the Ministry of Finance, the Public Procurement Office, the General Prosecutor's Office, the Anti-Monopoly Office, the Procurement Unit of the Deputy Prime Minister's Office, the Anti-Corruption Unit of the Government Office, and central contact point (CCP) OLAF for their participation and invaluable inputs for this strategy.

The OECD wishes to thank the international group of experts that contributed to the strategy and workshops, namely, Pilar Sáenz de Ormijana Valdés, Head of the Support Unit within the Anti-corruption Prosecutor´s Office, Spain, Declan Wylde, Head of Finance, Transport Infrastructure, Ireland, Simon Hannah, ESIF Compliance and Quality Assurance Manager, United Kingdom, Jo Kremers, Senior Audit Manager, Ministry of Finance, the Netherlands, Andris Kairišs, EU Funds Project Manager, Latvian School of Public Administration, Mark Schelfhout, Head of Unit Audit Shared Management I, DG Employment, Social Affairs and Inclusion, European Commission, and Rando Undrus, Anti-Fraud Advisor, Agricultural Registers and Information Board, Estonia.

Table of contents

Foreword 3

Acknowledgements 4

Abbreviations and acronyms 7

Executive summary 9

1 European Structural and Investment Funds in the Slovak Republic: An overview of the fraud and corruption risks 11
The ESI Funds project cycle and past challenges in the Slovak Republic 12
Fraud and corruption risks and schemes 14
The OECD partnership with the Central Co-ordination Body and the government of the Slovak Republic 15
Note 16

2 Enhancing fraud and corruption risk assessments in European Structural and Investment Funds in the Slovak Republic 17
Introduction 17
Priority 1 – Identify relevant risks by sharpening the focus on fraud and corruption 18
Priority 2 – Improve the precision and consistency of risk analysis and scoring 22
Priority 3 – Enhance the analysis of control activities when conducting risk assessments 24
Priority 4 – Make better use of national and external databases and data analytics to assess risks 27
Priority 5 – Improve use of the Arachne risk scoring tool to refine risk assessments 32
Notes 37

3 Adopting a systematic approach to managing fraud and corruption risks in European Structural and Investment Funds in the Slovak Republic 39
Introduction 39
Priority 1 – Develop explicit anti-fraud policies and foster a positive risk culture 40
Priority 2 – Establish a formal mechanism for co-ordination among authorities 43
Priority 3 – Increase the capacity to manage fraud and corruption risks with improved training 46
Priority 4 – Improve feedback loops with law enforcement authorities to enhance risk assessments 49
Priority 5 – Monitor and evaluate fraud risk management activities and controls 51

Annex A. A comprehensive fraud risk management scorecard for managing authorities 57

Annex B. The chronology of proposed actions for the Government of the Slovak Republic 60

References 61

Further reading 64

FIGURES

Figure 1.1. ESI Funds management 12
Figure 2.1. Risk management and assessment framework of an operational programme in the Slovak Republic 19
Figure 2.2. Linking inherent risk, residual risk and risk tolerance 25
Figure 2.3. Number of projects per project cost category and overall risk score 35

TABLES

Table 2.1. The scoring criteria for likelihood of a risk materialising in an operational programme 23
Table 2.2. The scoring criteria for risk impact on an operational programme 23
Table 2.3. Mapping of national data sources in the Slovak Republic for managing fraud and corruption risks 29
Table 3.1. Example of a fraud risk management scorecard for monitoring and evaluation 52

Table A B.1. Key actions for enhancing fraud and corruption risk assessments 60
Table A B.2. Key actions for adopting a systematic approach for managing fraud and corruption risks 60

Follow OECD Publications on:




http://twitter.com/OECD_Pubs


http://www.facebook.com/OECDPublications


http://www.linkedin.com/groups/OECD-Publications-4645871


http://www.youtube.com/oecdilibrary



http://www.oecd.org/oecddirect/

Abbreviations and acronyms

AA	Audit authority
AFCOS	Anti-Fraud Co-ordination Service
AMO	Anti-Monopoly Office
CA	Certifying authority
CCB	Central Co-ordination Body
CCP	Central Contact Point
CGET	Commissariat général à l'égalité des territoires (General Commission for Equal Territories) France
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CPO	Corruption Prevention Office
DPMO-II	Deputy Prime Minister's Office for Investments and Informatisation
EC	European Commission
EGESIF	Expert Group on European Structural Investment Funds, European Commission
ESI	European Structural and Investment (Funds)
EU	European Union
IBs	Intermediate bodies
GPO	General Prosecutor’s Office
IIA	Institute of Internal Auditors
IMS	Irregularities Management System
ISO	International Organization for Standardization
KR, KR 7	Key Requirement
M&E	Monitoring and evaluation
MAs	Managing authorities
MCS	Management and control system
NAFS	National Anti-Fraud Strategy
NKU	Najvyšší kontrolný úrad Slovenskej republiky (Supreme Audit Office of the Slovak Republic)
OLAF	Office européen de lutte antifraude (European Anti-Fraud Office)

OPs	Operational programmes
OTS	On-the-spot (checks)
PPO	Public Procurement Office
TFEU	Treaty on the Functioning of the European Union

Executive summary

Fraud and corruption threaten to divert taxpayers' money away from the key beneficiaries of public policies and investments: that is, our communities and citizens. When such risks materialise, citizens' trust in government declines and the consequences of fraud and corruption become acutely apparent. The European Structural and Investment (ESI) Funds, consisting of five structural funds designed to promote harmonious development across EU Member States, are a vehicle with enormous potential for economic growth and social development in the European Union. The volume of investment for 2014-20 is EUR 450 billion, including over EUR 15 billion for the Slovak Republic alone. Yet, these investments carry risks, including the potential for fraud, corruption and abuse.

For ESI Funds investments to achieve their policy goals, create jobs and promote a sustainable European economy, it is critical that governments have robust risk management policies, skills, and tools in place. With those prerequisites in mind, the strategy presented here provides targeted guidance for Slovak programme authorities on how to strengthen their practices in fraud and corruption risk management. The strategy identifies two key areas for improvement: 1) enhancing fraud and corruption risk assessments, with a focus on data-driven approaches**,** and 2) adopting a systematic approach to the management of fraud and corruption risks within ESI Funds.

Enhancing risk assessments

During the current programming period, managing authorities (MAs) in the Slovak Republic have made progress in developing their risk management frameworks and procedures for implementing operational programmes. Nevertheless, opportunities remain to improve fraud and corruption risk assessments further. The participating MAs have not accurately identified all relevant inherent risks, so that certain fraud and corruption risks remain undetected and unmitigated. To ensure that their risk management practices provide a strong basis for identifying all relevant fraud and corruption risks to ESI Funds, MAs can review and update their risk assessment processes and risk catalogues to ensure greater clarity and comprehensiveness. They can also improve the accuracy of their risk profiles by undertaking more robust risk analysis and scoring.

The *OECD Recommendation of the Council on Public Integrity* promotes taking a strategic approach to integrity, internal control and risk management. In the Slovak Republic, MAs can adopt strategic foresight for fraud and corruption risk management in ESI Funds. Notably, programme authorities can make better use of risk assessments, both as input to decision-making processes and to ensure that resources are allocated to areas prone to fraud and corruption. Furthermore, MAs do not take full advantage of data-driven approaches or tools. Making better use of both the Arachne risk-scoring tool and national databases could strengthen assessment of these risks.

Adopting a systematic approach to fraud and corruption risk management

MAs in the Slovak Republic have developed and adapted their procedures regarding fraud risk assessments in line with European Commission requirements. However, programme authorities can take steps to improve fraud and corruption risk governance and move away from current "check-the-box" approaches. For instance, in some MAs, risk management procedures do not incorporate any explicit focus on fraud and corruption, which leads to ad hoc approaches for managing such risks. Fostering a proactive risk culture can help MAs strengthen risk governance and embed fraud and corruption risk management into existing practices. This means going beyond the dissemination of codes and rules and communicating risk management values and principles to employees. MAs can establish or revise explicit anti-fraud policies to demonstrate their commitment to integrity and to communicate how specifically managing fraud and corruption risks can help achieve the objectives of operational programmes.

Enhanced co-operation and knowledge sharing are vital to ensure that programme authorities are maximising their skills and expertise to mitigate fraud and corruption risks. In the Slovak Republic, MAs do not regularly communicate with other authorities responsible for ESI Funds management or oversight, such as the certifying authority, Anti-Fraud Co-ordination Service (AFCOS), the audit authority (Ministry of Finance), or Corruption Prevention Office. Furthermore, MAs do not systematically communicate with law enforcement authorities such as the General Prosecutor's Office once cases of fraud or corruption have been referred to them. By establishing a task force within the AFCOS network and organising information-sharing forums, the government of the Slovak Republic can provide programme authorities with the means to improve their risk assessments and ensure that fraud and corruption risk management is embedded in authorities' practices.

The *OECD Recommendation of the Council on Public Integrity* underlines the need to provide those in the public sector with sufficient training and guidance in applying integrity standards in the workplace. Indeed, people and skills are the foundation of effective fraud risk assessments. With guidance from the Central Co-ordination Body, the Central Contact Point for the European Anti-Fraud Office can work with MAs to establish formalised and regular training to increase capacity for detecting fraud and corruption risks. Practical guidance on real cases and programmes, including with "red flags" and appropriate remedial actions, can be integrated into these training activities.

In the Slovak Republic, participating MAs are at the fifth stage of their risk management programmes, meaning they are embarking on the monitoring and evaluation process in 2019. All operational programmes can improve this process by placing greater focus on evaluating existing fraud and corruption risk management practices. For example, to enable benchmarking between MAs and continuously improve risk management, the Risk Management Working Groups can design scorecards with appropriate measurement criteria.

The high volume, complexity and value of investments through ESI Funds offer an attractive target for fraud and corruption in the Slovak Republic and other EU Member States. National authorities can work together to better manage fraud and corruption risks and safeguard integrity in ESI Funds. In doing so, governments could ensure that citizens reap the benefits of these investments in diverse sectors, and thereby foster trust in both government and ESI-funded programmes.

1 European Structural and Investment Funds in the Slovak Republic: An overview of the fraud and corruption risks

European Structural and Investment (ESI) Funds comprise the European Regional Development Fund, the Cohesion Fund, the European Agricultural Fund for Rural Development, the European Social Fund, and the European Maritime and Fisheries Fund. ESI Funds can support development and enhance the quality of life of citizens in the European Union – through investment in infrastructure, research and development, employment and training, agriculture, forestry and fisheries. With a budget of EUR 454 billion for the current programming period 2014-20, ESI Funds are the main investment policy tool of the EU (European Commission, 2015[1]).

Despite the significant benefits that these funds can bring, some countries have had to deal with cases of systemic corruption and fraud in their disbursement. Over the past four years, the European Anti-Fraud Office (OLAF) has investigated more instances of fraud and corruption involving structural funds than in any other area of the EU budget (Teffer, 2018[2]). According to the European Commission (EC), fraud against the financial interests of the EU amounts to about EUR 3 billion per year, roughly 2% of its annual budget (European Commission, 2018[3]). The European Regional Development Fund and Cohesion Fund are the funds most affected by fraudulent behaviour. Alongside direct financial losses, misuse of funds and fraudulent activity prevent operational programmes (OP) from reaching their objectives, and can create a culture of public distrust of institutions at both the national and EU level.

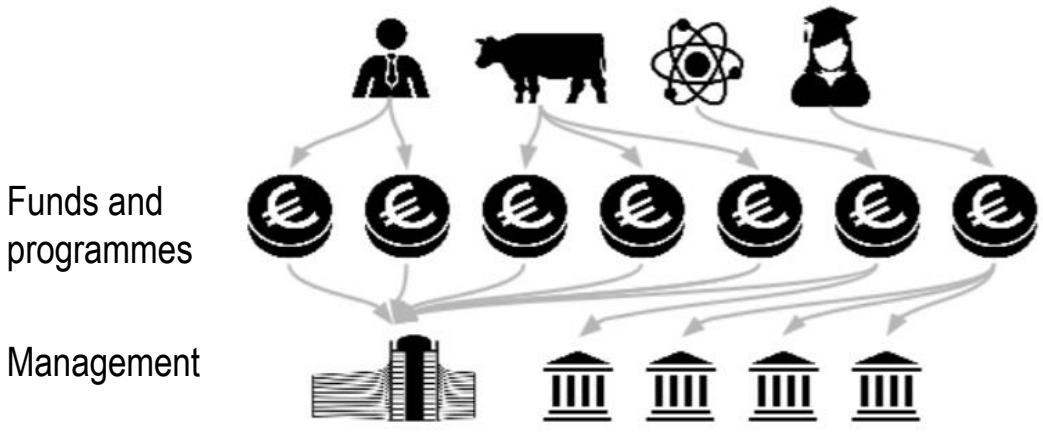
Fraud and corruption involving ESI funding have a direct negative impact on citizens across the EU. Funds can be recovered as a result of OLAF investigations, which means that projects linked to OPs may be suspended – or in some cases may never have a chance to be implemented, as indeed has occurred in the Slovak Republic. In 2016, OLAF recommended an amount of EUR 631 million (and in 2015, EUR 888 million) to be recovered (European Court of Auditors, 2019[4]). In these cases, citizens lose out on the benefits of projects that aim to improve socio-economic development across the EU, and countries may not be given future funding opportunities. Furthermore, fraud and corruption are perceived by many EU citizens as significant problems in relation to EU spending. In a recent Eurobarometer survey, 68% of the EU citizens responding think that corruption is widespread in their country (European Commission, 2017[5]). In relation to ESI Funds in particular, recent scandals in a number of Member States have drawn further attention to issues of fraud and corruption linked to the funds, causing public outrage throughout the EU. In 2017, Member States reported a total of EUR 320 million in fraudulent irregularities in the Cohesion Fund and European Maritime and Fisheries Fund alone (European Commission, 2018[3]). The size of the problem is further reflected in the investigative activities of OLAF: by the end of 2018, 73 of 362 ongoing investigations related specifically to ESI Funds (Teffer, 2018[2]).

The ESI Funds project cycle and past challenges in the Slovak Republic

ESI Funds provide support in delivering the Europe 2020 strategy of the EU, which centres on smart, sustainable and inclusive growth as a way to overcome structural weaknesses in Europe's economy. The funds should improve Europe's competitiveness and productivity, and underpin a sustainable social market economy (European Commission, n.d.[6]). As such, OPs in EU Member States are designed in line with the thematic objectives of the ESI Funds and the Europe 2020 strategy. The funds present opportunities for all Member States, but in Central and Eastern European countries in particular, the structural funds represent a significant incentive for public funding.

Once the budget, common rules, principles and priorities for each of the ESI Funds have been determined, the EC consults with Member States to produce a draft partnership agreement, while Member States also present draft OPs. The programmes are implemented by the Member States, which involves selecting, monitoring and evaluating hundreds of thousands of projects. This work is organised by managing authorities in each country and/or region: an MA may be a national ministry, a regional authority, a local council, or another public body that has been nominated and approved by the Member State in question. The EC pays the certified expenditure to each country and monitors each programme alongside the country concerned (Figure 1.1).

Figure 1.1. ESI Funds management



Source: Open Knowledge (2015), "Where does Europe's money go? A guide to EU budget data sources", https://community.openspending.org/resources/eu/pdf/WhereDoesEuropesMoneyGo.pdf (accessed 20 August 2019).

Grants from the funds are put towards specific projects or organisations in line with EU policies in different areas, such as agriculture, youth, and social inclusion, among others. To benefit from these grants, applicants must answer a call for proposal initiated by an MA. Once applicants respond to a call and submit an application, MAs undertake an initial assessment followed by a more comprehensive appraisal of the full application. If the application is successful at both stages, a funding agreement is drawn up specifying the terms of the funding. The successful applicant then becomes the grant beneficiary during the contract

management stage of the project cycle. Here, the beneficiary implements project activity in line with ESI Fund requirements, which are monitored by the MA. This includes checking claims and conducting on-the-spot monitoring visits to ensure that all the expenditure is within the stated rules. When the activity is completed, the MA conducts checks that the activity has closed and all the records are accurate and in place, as audits can continue to take place for years following completion of a project (Department for Communities and Local Government, 2015[7]).

Through nine national and regional programmes, the Slovak Republic has been allocated EUR 15.32 billion from ESI Funds for 2014-20. With a national contribution of EUR 4.72 billion, the Slovak Republic has a total budget of EUR 20.04 billion to be invested in different areas, from job creation and growth to supporting sustainable transport, as well as protecting the environment and investing in research and innovation. While all funds are designed to support the socio-economic development of the Slovak Republic, the following targets have been set for the current programming period:

- *Employment* – Support for 250 000 jobless people, particularly low-skilled workers and the long-term unemployed
- *Education* – Improvement of education and training through initiatives for over 100 000 pupils and students
- *Transport and infrastructure* – Reconstruction or renovation of 111 km of railways and 17 070 km of newly built roads, as well as the building or renovation of 157 310 square metres of public or commercial buildings
- *Social inclusion* – Support for 150 municipalities with the most deprived Roma communities
- *Firms* – Approximately 15 000 firms and 5 200 start-ups supported, with more than 6 000 new jobs created
- *Environment and energy* – Recycled waste increased by 197 466 tonnes a year and flood-protection measures benefiting 13 000 people
- *ICT infrastructure* – Broadband coverage and next-generation networks spread to 100% of 30 Mbit/s coverage
- *Research and innovation* – More than 1 000 new full-time researchers employed and 4 580 enterprises supported in order to introduce new products to the market
- *Public administration* – Up to 20 ministries to introduce quality management systems and develop training for civil servants to modernise public procurement.
- *Agriculture and rural development* – Modernisation of nearly 1 250 small and medium-sized farms to improve economic performance; financing of start-up costs for approximately 600 young farmers; more than 2 000 jobs created in rural areas; and designating 21% of total agricultural land to support biodiversity and/or landscapes (European Commission, 2014[8]).

In the Slovak Republic, ESI Funds have been a useful instrument for modernising infrastructure in, for example, the areas of education, social services, and civil structures and facilities in towns and municipalities. They have also enabled implementation of a number of major projects that could not have been possible without EU funding (KPMG, 2016[9]). As well as providing opportunities for Member States, implementing large amounts of EU funding can be a complex task that presents a number of different risks. The programming period 2007-2013 was affected by delays in setting up management and control mechanisms for OPs in the Slovak Republic, which resulted in a low rate of contracting that continued into the beginning of the current programming period. The government of the Slovak Republic has since taken steps to ensure greater transparency around management of funds, as well as simplified procedures.

However, the government faces persistent challenges in its management of fraud and corruption risks and prevention irregularities in implementing ESI Funds. Irregularities are not always fraudulent; they can indicate waste, mismanagement, or systemic problems in the Management and Control System (MCS)[1]. Fraudulent irregularities, on the other hand, are those that are committed deliberately. During the

programming period 2007-13, the following irregularities were reported most frequently and produced the most significant financial impact in the Slovak Republic:

- lack of transparency in the selection and evaluation of projects to be carried out within OPs
- infringement of procurement rules and procedures
- declaration of expenditure not in line with the actual works performed
- failure to ensure fair competition (Höslová, 2015[10]); (Government of the Slovak Republic, 2014[11]).

In particular, the Slovak Republic has experienced repeated deficiencies in relation to public procurement at the level of beneficiaries and insufficient verification by managing authorities. As discussed in the next section, fraud and corruption risks can manifest at each stage of the project cycle. In particular, the Slovak Republic and numerous other Member States have experienced challenges in mitigating risks in the project selection and implementation stages.

Fraud and corruption risks and schemes

Fraud affecting EU financial interests is defined in Article 3 of Directive (EU) 2017/1371 dealing with the fight against fraud by means of criminal law: it is characterised as a deliberate act of deception intended for personal gain or to cause a loss to another party (European Parliament, 2017[12]). A definition of corruption used by the EC is the abuse of public position for private gain. Types of fraudulent irregularities that are found in the implementation of OPs include, *inter alia*: falsified accounts/falsified supporting documents; missing or incomplete documents; infringement of public procurement rules; and unjustified expenditure. Both the EC and Member States must put in place measures to protect EU financial interests against fraud and corruption under Article 325 of the Treaty on the Functioning of the EU (TFEU) (European Union, 2016[13]).

In the course of the current programming period, the EC placed a stronger focus on fraud prevention in implementing ESI Funds in response to systemic challenges highlighted in previous programming periods. Specifically, many Member States have experienced cases of fraud and corruption in the project selection and implementation stages of the ESI-funded project cycle, potentially due to the number of actors involved in the management and delivery of OPs. Perpetrators have found ways to adapt their ploys not only to the ESI Fund context generally, but also to specific funds and OPs. Based on an OECD survey of over 80 practitioners from programme authorities in Member States, as well as interviews with experts, the main risks at each stage include the following:

- In the initial stage of the project cycle, potential fraud and corruption risks lie in both the application and project selection processes. For example, in an attempt to win projects and funds, an applicant may submit a false declaration to strengthen their application. In reality, the applicant may not possess the expertise or have the capacity to carry out the project properly. When it comes to project selection, an applicant may seek to influence members of the evaluation committee/board to ensure their project is selected. In some cases, applicants may even bribe officials. Alternatively, members of the evaluation committee/board may have a connection to and in some cases collude with the applicant to help them win the project. Fraud or corruption at this stage can have an impact throughout the project cycle, with perpetrators employing nefarious tactics in the later stages to conceal the original scheme.
- The fraud and corruption risks that arise during the project implementation stage are potentially due to the number of actors that can be involved. In addition, a number of procurement-specific risks are likely to arise at the implementation stage. For example, members of an MA or beneficiary may tailor tender specifications or leak sensitive bid information to favour one particular company or individual. Companies or contractors may also take part in collusive bidding in order to win tenders.

- Although the project closure and evaluation stages of a project carry fewer fraud or corruption risks, perpetrators may submit forged or falsified documentation to hide fraudulent or corrupt activity that took place earlier on in the project, ultimately allowing the activity to go undetected. In some cases, perpetrators may bribe or collude with auditors or evaluators to ensure that their reports and findings conceal the original fraudulent scheme.

Despite the focus of the EC and Member States on implementing anti-fraud measures during the current programming period as well as the subsequent one from 2021 to 2027, challenges remain with regard to fraud and corruption risk management. In an audit published in 2019 on tackling fraud in cohesion spending, the European Court of Auditors found improved fraud prevention measures in sampled MAs, but highlighted the need for further improvements to proactive fraud detection. Furthermore, the findings indicated that the MAs had not developed procedures for monitoring or evaluating the impact of their anti-fraud measures. Lastly, the audit found that the fraud detection rates published by the EC did not necessarily reflect the effectiveness of the detection mechanisms of Member States, or indicate how much fraud is actually detected. Instead, the rates showed how many cases Member States decided to report to the EC (European Court of Auditors, 2019[4]).

The OECD partnership with the Central Co-ordination Body and the government of the Slovak Republic

The Central Co-ordination Body (CCB), which sits in the Slovak Republic Deputy Prime Minister's Office for Investments and Informatisation (DPMO-II), plays a critical role in ensuring the principles of integrity, accountability and transparency in ESI-funded programmes. Established in June 2016, the CCB manages and co-ordinates the implementation of OPs among Slovak authorities. The CCB requested support from the OECD in improving the resilience of the ESI Funds environment and its ability to safeguard the funds from fraud and corruption. The CCB proposed four managing authorities to participate in the project that reflected a range of maturity and capacity for managing these risks. The four participating MAs are responsible for the following OPs: Quality of Environment; Human Resources; Integrated Infrastructure, and Research and Innovation. The policies, practices and insights from these MAs provided the basis for the analysis and actions in the strategy outlined here.

In addition to the aforementioned MAs, the CCB and the OECD engaged a number of other authorities in the Slovak Republic to ensure that the strategy takes into account the different responsibilities and experiences in managing fraud and corruption risks in OPs. Slovak authorities that participated in OECD missions and workshops, as well as providing documentation and inputs for the strategy, include: the Public Procurement Office (PPO), General Prosecutor’s Office (GPO), Anti-Monopoly Office (AMO), Procurement Unit of the Deputy Prime Minister’s Office, Anti-Corruption Unit of the Government Office, Ministry of Finance (certifying authority, audit authority), and central contact point (CCP) OLAF.

The OECD assessed relevant legislation, policies, practices and tools for managing risks, and organised five fact-finding missions, workshops and consultations with project participants. During the missions, experts and practitioners from Estonia, Ireland, Latvia, the Netherlands, Spain and the United Kingdom shared their experiences via practical case studies from their respective countries. For the fourth mission, the OECD team engaged an experienced representative from the European Commission to provide participants with a holistic view of the main challenges and opportunities for Member States regarding fraud and corruption risk mitigation in structural funding. In addition, the OECD conducted a survey of approximately 80 practitioners from programme authorities in other Member States to gain insights into the most prevalent fraud and corruption risks and schemes that other countries encounter throughout the ESI Funds project cycle. During Integrity Week 2019, the OECD organised a seminar with experts from Member States and EU-level institutions to gain their perspectives on different thematic areas that are

integral to this strategy. Last, the OECD team researched fraud and corruption schemes involving ESI Funds.

Reflecting the analysis and inputs from these efforts, the strategy is organised into two main thematic areas. The first is fraud and corruption risk assessments, with the focus on making better use of data. The second is fraud and corruption risk governance, including active co-operation among programme authorities, training and capacity building, co-ordination efforts, and finally, monitoring and evaluation (M&E) of fraud and corruption risk management practices. The proposed actions and priorities related to these areas build on the existing practices and capacity of the MAs and other project partners in the Slovak Republic.

Note

[1] Managing Authorities are required to set up a Management and Control System for their Operational Programme to ensure that projects are implemented with sound financial control. These systems aim to prevent, detect and correct any irregularities, and ensure the full legality and regularity of expenditure.

2 Enhancing fraud and corruption risk assessments in European Structural and Investment Funds in the Slovak Republic

Introduction

A comprehensive fraud risk assessment serves as a fundamental tool for safeguarding integrity in European Structural and Investment (ESI) Funds and fulfilling the objectives of operational programmes (OP). Managing authorities (MAs) in the Slovak Republic are required to conduct risk assessments in line with Article 125 paragraph 5, c) of Regulation 1303/2013 and to introduce adequate anti-fraud measures based on risk identification. The regulatory and policy frameworks offer MAs some flexibility in terms of tailoring risk assessments to individual contexts. Indeed, as illustrated in this chapter, the risk management practices of MAs reflect differences in environments, operations and programmes. These differences are particularly pronounced in risk assessments and risk catalogues.

While there is variation in how MAs manage and assess fraud and corruption risks, they face common challenges and share opportunities – such as the need to improve analysis of fraud and corruption risks and the possibility of making better use of data in this process. Developed from OECD interviews and research on the policies activities for risk management and control in the Slovak Republic, this chapter explores actions for the government to enhance its approach to managing and assessing fraud and corruption risks involving ESI Funds, focusing on the following key priorities:

- Priority 1 – Identify relevant risks by sharpening the focus on fraud and corruption
- Priority 2 – Improve the precision and consistency of risk analysis and scoring
- Priority 3 – Enhance the analysis of control activities when conducting risk assessments
- Priority 4 – Make better use of national and external databases and data analytics to assess risks
- Priority 5 – Improve use of the Arachne risk-scoring tool to refine risk assessments.

Priority 1 – Identify relevant risks by sharpening the focus on fraud and corruption

Issue analysis

Three of the four participating MAs formed risk management working groups. These working groups consist of members of different departments in MAs, experts from intermediate bodies (IBs), and representatives from paying units. The primary responsibilities of these working groups are to identify, analyse and evaluate risks; define existing control mechanisms; collect inputs from other units; monitor risks; and take mitigating actions. The risk management working groups generate a risk catalogue that summarises all possible identified risks, including fraud and corruption risks. To inform the risk catalogues, the working groups use historical knowledge and experience from the previous programming period, audit findings and media reports. The respective risk management procedures for different OPs also list several methodologies to support risk assessments, such as surveys and interviews.

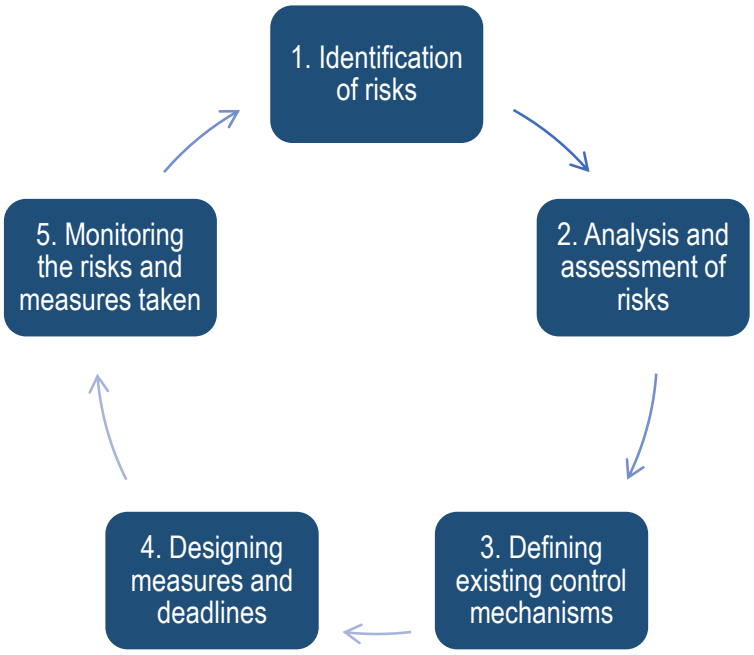
The OECD reviewed risk management and internal control policies, processes and procedures, risk catalogues, organisational charts, meeting minutes and other supporting documents from the four participating MAs. The review focused on the design of a fraud risk management framework and its application in the selected OPs. The MAs have established binding procedures for risk management, which articulate a methodology for the risk assessment process. The methodology incorporates guidance from the Expert Group on European Structural Investment Funds of the European Commission (hereafter EGESIF). Programme authorities can refer to EGESIF in several areas, including the overall Management and Control System (MCS), audit strategy, and management verifications to ensure proper implementation of OPs. In particular, guidance from EGESIF, including the *Fraud Risk Assessment and Effective and Proportionate Anti-Fraud Measures*, provides recommendations on how MAs can establish effective and proportionate anti-fraud measures based on risks (European Commission, 2014[14]).

As a critical first step, the four MAs that participated in the project had set clear objectives for reducing risks and mitigating their impact on strategic and operational goals of OPs. Their objectives included:

- building common awareness and understanding of risks across functions and departments within MAs;
- allocating resources more efficiently based on risks;
- ensuring effective functioning of the MCS in accordance with EU regulations and national legislation; and
- strengthening financial and compliance control processes within MCS to minimise the need for financial corrections.

MAs in the Slovak Republic have also established procedures for risk assessments that include identification of fraud risks. Risk assessment are critical tools for supporting MAs to identify, analyse and evaluate the likelihood and impact of individual risks, as well as interlinkages between risks across organisational objectives. The assessments help authorities to understand threats related to both internal and external environments, and then take stock of control activities and the effectiveness of mitigating actions. In general, risk management working groups in the Slovak Republic follow a similar assessment process, illustrated in Figure 2.1.

Figure 2.1. Risk management and assessment framework of an operational programme in the Slovak Republic



Source: Risk management procedures for the operational programme, Quality of Environment.

Risk assessments in practice are not always the linear process illustrated in the figure above. However, it is common for risk identification to begin with an assessment of inherent risks. Inherent fraud risks, or "raw risks", are assessed independently of relevant controls or mitigation measures. Their assessment typically involves an analysis, either qualitative (e.g. surveys, focus groups, interviews and desk research) or quantitative (e.g. statistical analysis and reviews of statistics and historical data), to understand their likelihood and impact. Identifying inherent risks requires an understanding of the universe of known fraud risks and the risk subgroups specific to each OP or MA. This activity benefits from the engagement of stakeholders with expert knowledge of different functions and sectors. After assessing inherent risks, a critical step is to then analyse and score the "residual risks," which is the risk that remains after an organisation has attempted to mitigate them in some ways. As part of this step in the assessment process, the likelihood and impact of each fraud risk after taking into account the control activities associated with a particular risk. The result of this assessment informs decisions about whether controls need to be adapted to mitigate risks in relation to a pre-determined risk tolerance, as discussed in more detail below.

The risk management procedures of MAs signal a commitment to meet EU requirements regarding the management of ESI Funds and align with international standards for risk management. Nonetheless, the MAs experience several implementation challenges, particularly with regards to assessing fraud and corruption risks. All four MAs referred to EGESIF when establishing their risk assessment practices, yet their risk mapping processes and outputs differ. Two of the four participating MAs use the fraud risk assessment template provided by the EC, which concentrates on anti-fraud measures. The other two MAs developed more comprehensive risk assessments and catalogues that cover many areas and processes, such as preparation, implementation, and monitoring and evaluation of an OP. These areas are then

divided into sub-areas – such as project selection and evaluation, public procurement, application for payment and project monitoring – for which particular risks are detailed. Project partners in the Slovak Republic indicated that these processes were also representative of other MAs. During this review, two key issues emerged:

- *A need to distinguish inherent fraud risks from other types of risks and control activities* – The fraud risk catalogues are broad and several representatives from MAs confused fraud risks with business risks, or categorised the root cause of risks as the risk itself. For example, some risk catalogues listed "insufficient verification of cost-effectiveness" and "inconsistent performance of expert evaluation" as inherent fraud risks. However, these are deficiencies that signal ineffective control measures or other types of risks. Including them in the inherent fraud risk category generated a lengthy and overly complex list of "risks" within some MAs. In another instance, an MA had difficulty distinguishing between fraud risk schemes and associated red flags. A red flag is a warning sign that fraud may have occurred, or will occur in the future. It is not evidence of fraud, but can draw attention to risks. A fraud risk scheme may be connected with a number of red flags and could require multiple controls. Confusion over risk concepts such as inherent risks, red flags, and mitigating controls indicates a need to increase knowledge for and capacity in application of risk assessment methodologies. Therefore, mistaking red flags and controls for risks can quickly expand risk catalogues. For instance, one OP identified and assessed 167 fraud risks and 327 total risks, including broader strategic and operational risks. Cumbersome, overly detailed risk catalogues require significant time to complete and can impede risk prioritisation while increasing administrative burdens.
- *A need to better assess fraud and corruption risks, taking into account the ESI Funds project cycle* – The catalogues from at least two MAs do not contain several fraud and corruption risks that threaten projects throughout the ESI-funded project cycle. For instance, these risk catalogues did not identify the various types of procurement risks for contracts tendered and managed by beneficiaries. Missing risks in some MA catalogues reflect the need to build knowledge and awareness of fraud risks and the related anti-fraud measures in specific OPs. The omission of critical risks also reflects the need to integrate different perspectives and competencies into the risk assessment process. During the existing identification phase, the chairperson of a risk management working group sends the members a template of the risk catalogue to fill in with potential risks. The members complete and submit the self-assessment document to the email address indicated within a specified period. The chairperson then creates a single risk catalogue for the OP based on the collective responses. The chairperson evaluates the information and decides whether to propose any new risks to be reviewed. Such survey-based assessments offer some benefits: a large number of employees can access and contribute to the process with fewer constraints, and assessment can be undertaken at a low cost. However, several issues can cause setbacks, such as limited follow-up, risk of misinterpreting responses, and individual responses received in isolation from others. As a result, MAs may miscalculate fraud and corruption risks if they overlook critical fraud and corruption schemes such as avoidance of competitive procurement procedures, collusive bidding, and manipulation of costs.

Key action: Review and update risk assessment procedures to ensure greater clarity for identifying fraud and corruption risks across the ESI Funds project cycle

The existing procedures of MAs can be amended to clarify the concepts of inherent risks, root causes, red flags and control activities. Developing and updating reference materials on common and actual fraud and corruption schemes, along with mitigating actions to detect and prevent risks, can also improve identification of inherent risks. For example, providing information on real cases that show the interconnected nature of fraud and corruption risks, schemes, red flags and control measures can inform the risk management working groups' activities at the stage of inherent risk identification. To this end,

guidance, reference materials and inputs to the risk management working groups could include the following components:

- prominent fraud and corruption risks across all stages of the ESI-funded project cycle, with a description of fraud and corruption schemes at each stage, submitted by managing authorities
- red flags for fraud and corruption risks at each stage of the project cycle, supported by data and indicators that can be used to detect them
- detailed case studies that demonstrate how a particular fraud or corruption operation was carried out, by whom, and how the fraud or corruption occurred
- good practices for preventing and mitigating fraud and corruption risks at each stage of the project cycle, including control measures and activities.

EC guidance places importance on including specific fraud risks identified through knowledge of previous fraudulent cases, as well as commonly recognised and recurring fraud schemes throughout all stages of the project cycle. The EGESIF guidelines on fraud risk assessments includes the fraud schemes and risks that are observed across OPs and EU Member States, including applicant selection, project implementation, and certification of costs and payments (European Commission, 2014[15]). According to EGESIF, MAs should adopt adequate preventive controls and detection measures, undertake thorough fraud risk assessments, provide timely responses to fraud risks and suspicions of fraud, and undertake investigations where appropriate. EGESIF also notes that anti-fraud measures should be proportionate to the risks identified.

MAs mostly adhere to and use the EGESIF guidelines as a baseline when developing risk assessments. Some MAs, however, have missed numerous significant fraud risks and schemes that are outlined in EGESIF and that may affect their OPs. To help focus the risk assessments, the MAs can review the identified risks against the recommended fraud risks in the EGESIF tool, and add other known risks for their specific OPs taking into account the ESI Funds project cycle, as illustrated in Chapter 1. However, it is critical that the MAs avoid simply replicating the risks in EGESIF and taking a “check-the-box” approach. Below are several common fraud and corruption risks identified by the OECD as having been omitted by at least two of the MAs.

Applicant selection stage

- Members of the MA or Evaluation Committees intentionally influence the selection of applications so as to favour certain applicants during shortlist approval and appraisal, influencing other decision makers in the process.
- An entity applies for funding for the same project from several EU funds without declaring multiple applications.

Implementation stage

- A beneficiary avoids the required competitive procedure to favour a particular applicant by splitting purchases, unjustified single source award (when contracts are awarded directly to a bidder without meeting the competitive requirements), avoidance of a tendering process or extension/modification of the contract to elude the re-tendering process.
- A beneficiary favours an applicant/tenderer because of an undeclared conflict of interest, bribes or kickbacks.
- A beneficiary favours a tenderer in a competitive procedure through rigged specifications, leaking bid data or manipulation of bids.
- Bidders manipulate a competitive procedure organised by a beneficiary to win a contract by setting up fake bidders, collusive bidding or creating phantom service providers.
- A contractor manipulates cost claims or invoices to overcharge or recharge incurred costs.

- A beneficiary violates the contract conditions by non-delivery of the agreed project due to the non-existence of products or underperformed operation in relation to the agreement.
- A contractor intentionally overstates the activities of provided personnel to claim them as eligible costs or a beneficiary knowingly claims false labour costs not in line with the contract.

Certification/payment stage

- Expenditure may be validated by a certifying authority that has a connection to the beneficiary, resulting in conflict of interest.

The list above is not exhaustive. Beyond EGESIF, there are opportunities for MAs to update their risk catalogues to focus on the most common and severe types of fraud and corruption risks. The list should not be too extensive: a "reasonable" number of risks is subjective, but as a guiding principle, the risk catalogue should promote a concise overview of material risks linking to the broader objectives for managing fraud and corruption risks with ESI Funds. MAs can introduce other methods of conducting risk assessments and understand the root causes of risks to complement the existing survey-based electronic process. For instance, various tools can support the MAs and OPs to assess internal and external context, as well as the root causes of risks to better understand why a risk occurs.[1] Such tools can help to promote communication among stakeholders from different ministries and teams. Similarly, increased use of interviews would also promote engagement with key stakeholders, and allow risk managers to ask follow-up questions, probe for underlying issues, and increase foresight regarding potential future events. Facilitated workshops can foster exchange among experienced participants, potentially uncover hidden risks, and build consensus around risk prioritisation. Chapter 3 delves more deeply into the priorities and key actions for developing skills and knowledge.

Priority 2 – Improve the precision and consistency of risk analysis and scoring

Issue analysis

The four MAs have a similar risk assessment and scoring process. In general, the risk management working groups within MAs analyse and evaluate the likelihood and impact of risks, and then determine the overall risk level and mitigating controls. The MAs assess several key characteristics of each risk, including:

- the relevance to fraud, taking into account EGESIF recommendations;
- the type of environment from which the risk arises;
- potential risk owners;
- the risk impact, i.e. the degree of severity of the negative impact; and
- the likelihood of the risk.

The OECD reviewed the assessment processes and scoring of the four MAs, and noted several differences that indicate a need for better coherence and consistency of approaches between MAs. For instance, two MAs employ a five-by-five risk matrix, one MA uses a four-by-four risk rating scale, and the remaining MA chooses a three-by-three risk scoring system. A more consistent rating method may better facilitate benchmarking and exchange of good practices concerning risk assessments among OPs. The MAs' procedures also summarise several techniques of risk analysis they employ – such as risk sensitivity analysis, which explores various possible risk scenarios, and event tree analysis, which is used to evaluate a process and related events that could generate risks. However, the procedures have limited information on conducting these techniques, which contributes to knowledge gaps and inconsistent implementation among MAs.

Current risk catalogues do not contain any detailed analysis for explaining the scores for the two risk attributes. Three of the four MAs only define the likelihood and impact of risks in general terms, without explicit criteria for scoring fraud and corruption risks. In addition, the current methods of risk analysis do not address the interrelationships between risks arising at different stages of the project life cycle. When potential events are correlated, risk managers should assess the *combined* effect, because the link among risks could alter their likelihood and impact (COSO, 2016[16]). For example, detection of fraud risks, such as tailoring call specifications at the project initiation stage, can often help prevent related risks arising in subsequent stages. In addition, MAs could clarify the extent to which they consider changes in internal and external contexts when assessing risks, and tailor risk rating criteria to the realities of specific OPs. The drivers and root causes of fraud and corruption risks in OPs can depend on a myriad of factors, such as the sector to which the OP relates, the actors involved in its implementation, or even the geographical location of the project.

Key action: Clarify and improve the criteria for scoring fraud and corruption risks

To build on existing efforts, MAs can provide guidance and develop criteria for scoring fraud and corruption risks. The values assigned to the likelihood and impact are essential inputs for assessing and managing risks. Therefore, clear instructions are critical to ensure that risk profiles are accurate and to promote consistent risk assessments among the risk management working groups. One MA provides a practical example of what the scoring criteria could involve (Table 2.1 and Table 2.2).

Table 2.1. The scoring criteria for likelihood of a risk materialising in an operational programme

Likelihood assessment	Description	Likelihood of a risk materialising
3	High likelihood	The event is expected to occur in most cases during the 7-year programming period.
2	Medium likelihood	The event is expected to occur in some cases during the 7-year programming period.
1	Low likelihood	The event is expected to occur in exceptional cases during the 7-year programming period.

Source: Risk Management Procedures for Operational Programme Integrated Infrastructure.

Table 2.2. The scoring criteria for risk impact on an operational programme

Impact rating	Operational objectives	Financial objectives	Compliance objectives
1	If the risk materialises, it will have little or no impact on the successful implementation of the OP and the related projects.	If the risk materialises, it will have little or no financial impact on the successful implementation of the OP and the related projects, in the form of non-reimbursement or financial corrections.	If a risk materialises, it will have little or no impact on the successful implementation of the OP and the related projects in terms of compliance.
2	If the risk materialises, there is nevertheless a relatively high likelihood that the objectives of the OP will be achieved; may have a negative impact on the objectives of some individual projects.	If the risk materialises, it will not affect the achievement of the financial objectives of the entire OP, although it may have a financial impact on some projects.	If the risk materialises, the compliance objectives will not be affected while some individual projects may face minor compliance issues.
3	If the risk materialises, the operational objectives of the OP will most likely not be achieved.	If the risk materialises, the financial objectives of the OP will most likely not be achieved.	If the risk materialises, the compliance objectives of the OP are unlikely to be achieved.

Note: The impact assessment is based on assessment of the risk in question.
Source: Risk Management Procedures for Operational Programme Integrated Infrastructure.

The scoring system above is a simple, but effective, starting point that MAs can supplement with additional considerations of known risk factors for fraud and corruption. For instance, guidance materials can cover additional factors and questions when assessing the likelihood that a fraud risk will emerge, such as:

- *Complexity* – What is the complexity of activities involved in the process being analysed? Do they introduce any vulnerabilities?
- *Vulnerability* – How vulnerable is the area in the project cycle to fraud and corruption? Is there obtainable information or knowledge of beneficiaries based on previous projects? Have there been any significant changes made to the funded activities?
- *History* – How frequently has this fraud or corruption scheme occurred in the past? What do historical risk data indicate?

Two common pitfalls that undermine risk assessments are the failure to include relevant stakeholders in the process, and inadequate consideration of insight from experts who have experience in dealing with fraud and corruption. Effective risk analysis of the impact and likelihood of risks requires dialogue beyond compiling risk scores from working group members. When analysing qualitative information, staff within MAs should document the nature, root causes and drivers of identified risks to support risk scores. Risk management functions can also improve qualitative analysis by drawing upon quantitative data. Priority 3 in this chapter will delve deeper into this issue, exploring practical ways to develop data-driven approaches for fraud risk management.

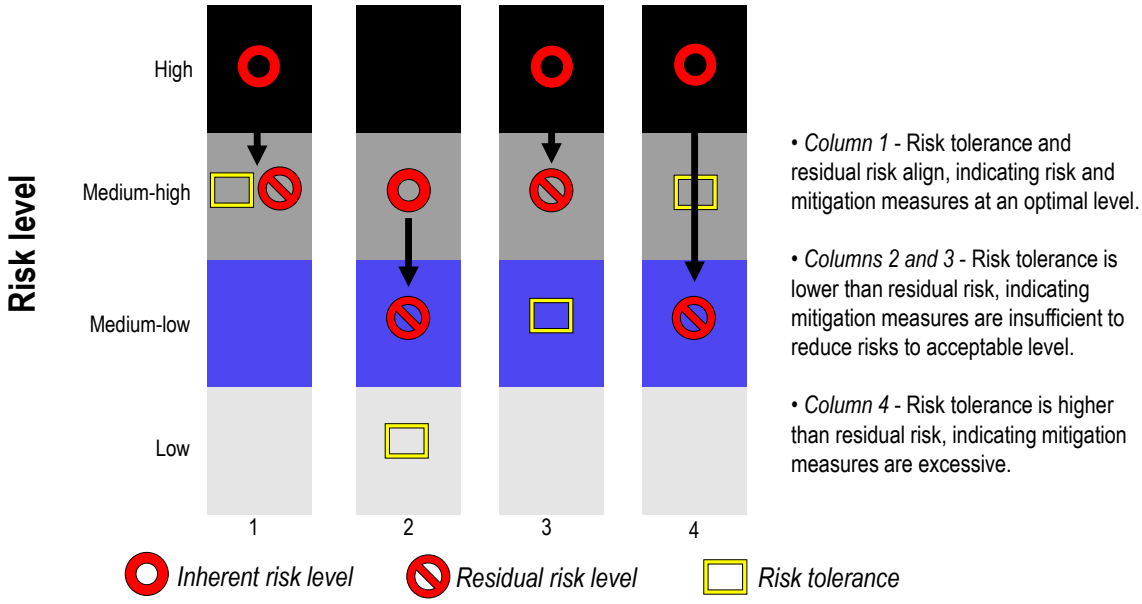
Priority 3 – Enhance the analysis of control activities when conducting risk assessments

Issue analysis

The MA's risk management procedures specify that the working groups or another responsible risk management function in MAs should determine whether controls reduce risks to an acceptable level. The MAs determine what is "acceptable" and define their risk tolerances for each risk accordingly prior to the risk identification process. Risk tolerance is a critical concept in risk management. It represents the level of risk that managers are willing to accept after implementing control activities, and therefore it helps to guide officials in their decisions to accept, reduce, avoid or share risks. The institution's overall objectives and resources are other factors that influence determinations about the level of risk tolerance.

The European Commission's *Guidance Note on Fraud Risk Assessment and Effective and Proportionate Anti-Fraud Measures* notes that "all programme authorities should be committed to zero tolerance to fraud, starting with the adoption of the rights tone from the top" (European Commission, 2014[14]). "Zero tolerance" can indeed be a compelling message for promoting the right tone to support a culture of integrity, but risk tolerance serves a practical purpose for assessing inherent and residual risks, as illustrated in Figure 2.2 below. In general, all MAs should have a low tolerance or risk threshold for fraud and corruption and should seek to maintain residual or net risks at a perceived level of low (or "very low").

Figure 2.2. Linking inherent risk, residual risk and risk tolerance



Source: Adapted from UK HM Treasury, 2016.

The MAs state their risk tolerance in their risk management procedures; however, a review of the MAs' risk catalogues and discussion with officials indicated a disconnect between the stated risk tolerances and control activities. Moreover, for several MAs, some of the controls documented were not appropriate for the identified fraud schemes. For instance, controls like separation of duties or the four-eye principle—where a certain activity, decision or transaction must be approved by at least two people—are at best insufficient and likely ineffective for mitigating the risks of fraudulent applications or collusive bidding. Incomplete or inaccurate assessments of control activities, without proper linkage to risks and risk tolerances, can undermine the risk assessment process and ultimately lead to gaps in treating fraud and corruption risks. Moreover, several MAs do not regularly evaluate controls at all to determine if they are effective. Consequently, the risk management working groups may inaccurately assess the effect of controls in reducing risks, or overlook risks altogether.

Another related challenge facing the MAs is that in some cases control measures are not proportionate to the assessed risk levels. At present, most projects and beneficiaries undergo the same verification procedures and control checklists as part of the compliance-oriented "zero tolerance" regime, regardless of the level of risks. Fraud and corruption risks with greater impact and likelihood do not necessarily trigger responsive, proportionate control measures. To lessen the probability of certain fraud and corruption risks materialising at subsequent stages of the project cycle, it is critical for MAs to assess and monitor the proportionality of controls.

Key action: Ensure control activities are appropriate, sufficient and proportional for mitigating identified risks

MAs can improve the risk assessment process and the clarity of risk catalogues by ensuring that control measures adequately address the identified fraud and corruption risks. The key action under Priority 2, developing guidance that includes detailed information on common fraud and corruption schemes along with descriptions of mitigating controls, can contribute to this. Moreover, MAs could draw from the

experience of other Member States. The OECD conducted a survey on practices for managing fraud and corruption risks in the European Union; 79 programme authorities from the 28 Member States participated. The responses indicated that false declarations submitted by applicants and conflict of interest within evaluation committees, which is responsible for appraising and choosing applications, pose some of the highest risk when selecting applicants. To inform improvements to MAs' controls in these high-risk areas, they could ensure the following activities, employed by MAs in other Member States, are effectively designed and implemented:

- A standard documented process for the selection of projects based on agreed criteria. Staff with the appropriate skills and experience review the outline and full applications, following the established assessment and appraisal processes. There should be greater scrutiny and review for quality assurance.
- A conflict of interest policy, including an annual declaration and register for all employees, and has measures in place to ensure that these are followed and checked.
- All applications are recorded and appraised in accordance with pre-determined criteria. Furthermore, all decisions on acceptance or rejection are communicated to the applicants.
- The evaluation committee provides advice on whether proposed activities meet strategic needs, provide good value for money, and are consistent with the defined priorities. These discussions are fully documented.

Furthermore, the OECD survey and follow-up interviews with practitioners suggested that manipulation of competitive procurement procedures and submission of fraudulent documents is another high risk, occurring most often during the project implementation stage.[2] To mitigate these risks, controls must be specific and targeted to address the various types of fraud and corruption schemes. Practitioners from EU Member States rated the following controls, some of which are reflected in EGESIF, as the most effective means for reducing risk exposure when tendering and managing contracts:

- The MA recommends that at least two staff members sign off procurement scoring documentation, and evidence of tenders is tested during on-the-spot (OTS) checks.
- The MA requires the beneficiary to provide information on the procurement process, including details regarding whoever carried out the tender process.
- The MA performs management verifications before certification and confirms that the beneficiary has adequate controls applied to the procurement process, including bidding procedures.
- The MA is furnished with guidance that clearly contains a requirement for any single source awards (otherwise known as direct contracts) to be reported to the MA with detailed justification.
- The MA seeks further evidence and information regarding any additional works, and tests whether or not these have been awarded correctly during OTS checks.
- The MA ensures a transparent bid process and reviews the operation of related controls for a sample of beneficiaries.
- The MA reviews contract awards and verifies the tendering process during on-the-spot checks for a sample of projects.

Early detection of fraud and corruption risks can enable MAs to implement appropriate and proportional measures that reduce the likelihood of similar issues arising later on in the project. MAs in the United Kingdom, for example, assess fraud and corruption risks, check for relevant controls at all stages of the project cycle and encourage early intervention, which helps to mitigate risks in the later stages of project implementation (see Box 2.1). Various measures can be applied in the Slovak Republic to strengthen the detection of fraud and corruption in the preliminary stages of the project cycle. Currently, MAs analyse risks before the final approval of a call for proposals. The risks they consider mainly focus on implementation failures, such as selecting inappropriate conditions of applicant eligibility or excluding value-for-money criteria. MAs risk analysis can account for fraud and corruption risks before approving

calls for projects, including assessing conflicts of interest, undermining of merit-based procedures, tailored call specifications and vague criteria. MAs can also introduce additional checks to detect and prevent risks like nepotism and conflict of interest at the project development phase when they score, review and select applicants. At this stage, MAs can also begin to consider fraud and corruption risks that are specific to procurement processes, and identify high-risk partners and subcontractors who may be involved in multiple ESI-funded projects.

Box 2.1. Project Inception Visits in the United Kingdom to detect risks and check controls at an early stage

In the United Kingdom, MAs consider potential fraud and corruption risks at all stages of the ESI-funded project cycle, including initiation, development, delivery and closure. Threats such as conflict of interest, manipulation and collusion may exist throughout the cycle, but different triggers and thus controls will apply at the various stages. For instance, before a project commences, staff from the MA will initiate a Project Inception Visit. These visits are an essential first step in checking that beneficiaries have in place the necessary audit systems, human resources, financial arrangements and processes to deliver a project compliant with requirements. In line with control procedures, employees carrying out the visit must fill in a form to document and verify controls – including project management and governance, financial control, verification of expenditures, counter-fraud policy and processes, and compliance with procurement regulations. Any findings at this stage can help identify risks and allow MAs to follow up with the beneficiaries to address any significant deficiencies at the early stages of implementation.

Source: Developed from OECD mission to the Slovak Republic, February 2019.

Lastly, relevant units from MAs could better monitor and test selected controls, particularly in areas facing higher risks, to verify that they are designed properly and are functioning efficiently. Given the fact that multiple personnel and various entities within and outside of the MAs are involved in risk mitigation measures, there should be clear communication of how to evaluate the effectiveness of controls in the relevant procedures and guidance. The testing of control quality also serves to provide evidence of how effectively controls mitigate risks, which should be properly communicated to all risk owners.

Priority 4 – Make better use of national and external databases and data analytics to assess risks

Issue analysis

National and external databases and systems can provide insights into fraud and corruption risks across OPs, and provide systemic monitoring and reports for Anti-Fraud Co-ordination Service (AFCOS) network partners. MAs use several systems such as ITMS 2014+ (ITMS), the Irregularities Management System (IMS), procurement databases and company registers. ITMS is a national system that supports ESI-funded projects and serves as a central registry for a project's monitoring, control, and financial management. The Deputy Prime Minister's Office for Investments and Informatisation (DPMO-II) and the Central Co-ordination Body (CCB) are the owners of this system. Central Contact Point (CCP) OLAF reports irregularities in ESI Funds implementation to IMS based on the data provided by certifying authority (CA) and information recorded by MAs in ITMS. Irregularities are reported to OLAF through IMS on a quarterly and monthly basis in accordance with relevant EU legislation. The Public Procurement Office (PPO) makes available several procurement databases, including a registry of contracts, the profile of contracting authorities, compulsory disclosure of information and a registry of beneficial owners. Company registers

feature data on change of ownership and management, financial performance and company assets. The Ministry of Justice maintains and updates the registers.

The detailed information ITMS generates on ESI-funded projects includes irregularities (including suspected fraudulent irregularities), project background, applicable laws/acts, and a probable sum of funds connected to an irregularity. Project managers also use other databases to assist with management verifications. However, the data from these national systems are not extensively used for identifying and assessing fraud risks in the Slovak Republic. And while MAs, CA and other programme authorities apply national tools including ITMS and public procurement databases, they do not do so on a systematic basis. The databases contain information valuable for detecting different types of fraud and corruption schemes. ITMS, for example, can help identify double funding and manipulation of project costs. Data from company registers combined with the registry of beneficial owners can be used to detect risks of conflict of interest. Procurement databases that are not currently being used, on the other hand, could reveal red flags for collusive bidding and manipulation of competitive procurement procedures. Furthermore, system-level risk analysis and reporting related to fraud and corruption risks in ESI funds covering all OPs are not currently undertaken. Nor do MAs share reports or indicators related to fraud and corruption.

Examples can be drawn from other EU Member States to demonstrate how these databases can be used to monitor fraud and corruption risk trends at the national level. In Croatia and the United Kingdom, for example, authorities that maintain the national tools for tracking ESI-funded projects and recording irregularities define granular data fields to capture relevant information, including business processes, sources, sectors, geographical location, beneficiaries, types and causes of irregularities, and resulting fraud. The MAs together with the AFCOS authority review and discuss the aggregate trends and statistical analysis of these cases to identify the riskiest areas in the country. In the Czech Republic, several MAs adopted a common approach to integrating red flags to monitor fraud risks in project management with a mechanism called risk cards. A national system helps these MAs assess and quantify the probability of fraud emerging and the associated impact through the use of a risk card, along with the red flags (PWC, 2018[17]). As a result, each individual project has an accompanying risk profile and a description of the risk management approach, including planned verifications throughout the different stages of a project. The central authorities therefore have access to a holistic view of the total risks based on a selected portfolio of projects.

Key Action: Develop a plan for more effective use of data on irregularities and public procurement

The OECD recognises a valuable opportunity in the Slovak Republic to review and revise available national tools and data sources, including ITMS, IMS, and public procurement databases consisting of company and beneficial ownership registers. A preliminary mapping of data sources is provided in Table 2.3.

Table 2.3. Mapping of national data sources in the Slovak Republic for managing fraud and corruption risks

Databases and tools	Data owners	Data users	Data fields used and information	Challenges participants reported having experienced
Company registers (www.orsr.sk)	Ministry of Justice	MAs and CA	Changes in senior management, owners and structure of a company	Effective use of the information
Public procurement databases	Public Procurement Office	MAs and CA	Published tenders, FAQs and cases identified with discrepancies	System application in the field of control
ITMS 2014+	CCB/DPMO-II	MAs, CA and AA	All projects, beneficiaries and contractors are recorded in the system, which flows through the cycle of ESI-funded projects.	Informing other databases and useful matching and cross-referencing with other data sources
Irregularity management system (IMS)	CCP OLAF	CCP OLAF, CA	All types of irregularities above EUR 10 000 euros are reported	Information contained in an annual report to OLAF but not used in trend analysis for the Slovak Republic
Audit and control findings	Ministry of Finance	MAs and CA	All audits performed since 2009 and the database allow historical comparison of results and reports	Finding appropriate measures to monitor in evaluating fraud risk assessments
Anti-Monopoly Office online databases	Anti-Monopoly Office	MAs and CA	Limited public info on anti-competition cases with restrictive access to sensitive data such as state aid schemes	Ensuring red flags related to anti-competition are incorporated in fraud and corruption risk analysis (i.e. of rigged bidding and collusion)
Social security agency data	Not available	MAs	Not publically available but MAs can obtain access during the project approval process	Data currently used only on a single project basis
Supreme Audit Office online databases	Supreme Audit Office	CA and AA	Audit reports, opinions and findings issued by the Supreme Audit Office	Reports are not regularly consulted

Source: Databases and tools were reported by selected managing authorities in a survey, and additional information was acquired during a workshop undertaken by the OECD in Bratislava, May 2019.

As previously noted, the ITMS 2014+ system provides a wealth of data for fraud risk management activities: information on calls for proposals, applications for grants, projects, irregularities, public procurement, suppliers, and requests for payments. No defined plan for taking a data-driven approach to complement existing qualitative risk assessment is in place to guide government entities to extract meaningful data from these sources through analysis, tools or techniques. Consequently, opportunities to utilise data and enhance data analytics for safeguarding ESI Funds against fraud and corruption may be overlooked.

The creation of a data-driven risk assessment plan is critical in enabling MAs and other programme authorities to improve their use of data to prevent and detect fraud and corruption. Furthermore, by improving data governance, data management, and analytics in the context of corruption and fraud risk assessments, MAs can benefit from positive spill over effects to enhance the use of data to advance other objectives, such as identifying and assessing strategic and operational risks.

Data governance can drive the improved use of data to assess fraud and corruption risks in ESI Funds, in particular, the risk identification and analysis stages. When developing a plan for taking a data-driven approach, key areas to take into account include the following:

- *Institutional and data governance* – Various institutional factors can influence the use of data analytics and the readiness of a government entity such as MA to apply data-driven approaches for identifying, analysing and assessing fraud risks. A plan for improving the use of data, therefore, also needs to consider these major factors and the associated limitations in the long term in order

to establish realistic expectations about what can be achieved for the use of data and data analytics in the Slovak Republic. The mandate and policies can show senior management's support for data analytics and assign clear roles and responsibilities. The top leadership can demonstrate that they value data analytics by requiring data to be presented to make major decisions. Since many stakeholders use systems such as ITMS, consistent and comprehensive data governance needs to provide standards and controls that will help ensure availability, consistency, security and integrity of data. Ongoing measures by the CCB to provide more open data and to enhance data quality can allow better use of structured data from the system. Effective governance enables access to and sharing of data and establishing co-operative relationships among entities, including for example data producers such as the CCB and PPO and data users such as MAs and IBs.

- *People and skills* – Skills and knowledge to apply appropriate methodologies and analytic techniques are critical. ESI fund authorities can evaluate several criteria including staff backing, people resources and leadership buy-in, to gauge the organisational readiness. Furthermore, data analytics for assessing fraud and corruption risks require inputs from individuals with anti-fraud experience and sector-specific knowledge. For instance, fraud and corruption risks in the education sector can be different from those in the renewable infrastructure sector, where schemes and operations carry distinct levels of complexity. Risk management expertise can also complement the process of integrating data analytics with established risk assessment methodologies. Government entities that employ data analytics on a more advanced level can also informally share good practices with other authorities. One MA recently created an analytical unit to establish good practices of data analysis – an effective way to group resources together to develop the in-house technical capability for analysing data. This new structure also allows investing in specialised staff with training to promote more data-driven risk analysis.
- *Technology* – Technological infrastructure, tools and software underpin many of the processes for effective data-driven risk assessments (OECD, 2019[18]). The MAs and relevant authorities can co-ordinate and adopt a strategic approach to investment in infrastructure that supports data analytics, aligning investments with objectives. The technology should match the available skills of the staff to employ the tools. Open-source solutions and free third-party tools sometimes can sufficiently meet the needs of technological infrastructure before the personnel move to a more advanced stage of data analytics.

In addition to considering the elements above, a data analytics plan for making better use of data also needs to articulate a concrete application. In the context of individual fraud and corruption risk assessments, data is particularly useful for risk identification and analysis. Defining the specific uses during the risk assessment processes helps to link the plan to specific activities and defines a manageable scope that reflects policies and processes that are familiar to stakeholders. It also allows individual MAs to tailor the plan to their specific contexts for conducting risk assessments. The OECD has developed guidance that identifies good practices to support government entities to conduct data-driven risk assessments to safeguard integrity (OECD, 2019[18]). Programme authorities can draw lessons from the guide for integrating data into their risk assessment processes further. The steps below are not necessarily sequential, and they are often iterative. For instance, objectives can direct the MAs towards a specific source of data for understanding fraud and corruption risks, but issues with data availability or quality can also change the scope of those objectives. Moreover, the steps should be refined based on the selected phase of the risk assessment process. The MAs decisions about when and how to incorporate an analytics capacity within the risk assessment process, such as risk identification, analysis, or scoring, would influence the practical application of these steps. These steps are simplified for illustrative purposes, and are primarily meant as a starting point to inform the strategic thinking of the CCB and MAs in this area:

- *Define objectives* – The ultimate aim of a data-driven approach is to enhance risk assessments, which can inform decision making – for example, decisions about types of preventive actions to take to respond to risks and adapt controls. Ongoing risk assessments aid in developing questions

about hindsight, insight, and foresight so that risks steer the objectives of the data analytics as opposed to having tools and data drive the questions. For example, some questions that data analytics can help answer are the particular suppliers and sectors that present the highest fraud risks, or those phases of the ESI Funds project cycle that appear to pose the greatest corruption risks and why. Data analytics can help MAs establish where risks are and determine with greater confidence the impact and likelihood of the identified fraud and corruption schemes. However, further review, investigation and a court ruling are required to ascertain whether fraud or corruption occurred. The objective of data analytics in risk assessments is primarily preventive, and offers the prospect of detecting high-risk cases for referral (OECD, 2019[18]).

- *Identify data needs and sources* – Once objectives are defined in alignment with the identified fraud and corruption risks, the next step is to look for the data that will illuminate these risks and locate the related data sources. These sources could be within the MAs, in other government institutions, or be from external, non-governmental organisations. The ITMS and IMS both depend on inputs by the MAs, IBs, CAs, and AAs regarding each project. The source of procurement information on open tenders originates from the publicly open data released by PPO.
- *Obtain and understand data and evaluate its quality* – The next step involves collecting the data and testing its quality, including usability, consistency, completeness and reliability. This stage is essential for understanding and evaluating data obtained from external entities. Sometimes, the formats of data from various sources can be unstructured or incompatible, a situation that may lengthen the time required for data cleaning. Analysts can apply validation tests to verify and ensure data quality. Any discrepancies should be addressed before moving to the analysis. A third-party service provider – such as for example the ITMS tool – could also perform this step, to ensure the data's quality.
- *Develop an analytical approach and perform the analysis* – At this stage, an analytical approach is needed; the plan should describe the data to be analysed, the specific analytics methodologies to be conducted, and the frequency of analysis. The MAs and relevant authorities should plan to analyse all relevant data and design data analytic procedures based on the identified fraud indicators. They also need to determine if analysis should be performed on an ad hoc, periodic or continuous basis. Whenever possible, specific analytic tests can be automated to create efficiencies for future study. Various software programmes can facilitate analyses. These can be simple tools such as Microsoft Access and Excel for analysing the trends of irregularities and potential fraud types. Alternatively, a more sophisticated data analytics team can also use other software programmes (e.g. SAS and open-sourced languages such as R and Python) to process more massive databases and employ complex techniques such as text analysis and predictive modeling. In the Slovak Republic, these suggested opportunities for improving the use of data analytics for fraud risk assessments already comprise the necessary tools for analysis without the need to design new analytical methods from scratch. Therefore, MAs and relevant authorities, including the CCB, can implement the recommended actions with minimum technical barriers.
- *Interpret, communicate and act* – Finally, MAs need to interpret the results in order to answer the questions set in the initial objectives. Data analytics do not confirm fraud incidents but signal specific cases that are more prone to certain fraud and corruption risks. Furthermore, the results can also uncover patterns and trends, which are useful in assessing risks in OPs and at system level across the MAs. Data visualisation tools such as dashboards, maps and charts can point out areas with higher risks, help communicate the findings, and propel remediating actions at both OP and system levels.

Key Action: Conduct periodic statistical analysis of irregularities, fraud cases and audit findings to help determine higher-risk areas in different sectors across the whole system

MAs, with the support of CCP OLAF, can conduct periodic statistical analysis of irregularities, suspected fraud, corruption investigations and audit findings to help determine higher-risk areas in various sectors. This analysis can better pinpoint specific fraud and corruption activities or beneficiaries that pose higher risk. To take fuller advantage of insights from audit bodies and with support from the new task force dedicated to fraud risk management, MAs can develop new approaches to compiling and analysing pertinent data from audit reports, and thereby build institutional knowledge and awareness across the national system. This includes gaining insights from the fraud and corruption risks uncovered by the MA, as well as data on how effective their fraud risk management activities and controls have been at preventing and detecting fraud and corruption over time. In the United Kingdom, MAs make use of audit reports to identify common trends in fraud and corruption schemes during the previous quarter, as well as to assess how well their anti-fraud measures are functioning. For example, audit reports for one OP indicated that the MA needed to carry out more rigorous testing and due diligence checks on grant beneficiaries to mitigate conflict of interest risks. As a result, the MA is now testing the conflict of interest registers more frequently. Crucially, analysis of audit data, along with data from other internal and external sources (detection tools, reporting mechanisms, media reports), allows managers to prioritise and take corrective actions where necessary (GAO, 2015[19]).

Priority 5 – Improve use of the Arachne risk scoring tool to refine risk assessments

Issue analysis

As discussed, the approach to risk assessments of the four MAs participating in the OECD review is qualitative, based on the perceptions of the risk management working groups and input from key employees. In its guidance, the EC encourages the use of data analytics to enrich the risk assessment process, and in particular the use of Arachne, a web-based tool with data on contractors, contracts, beneficiaries and projects (European Commission, 2014[14]). Arachne became operational in 2013 as a tool to support authorities of EU Member States to identify and prioritise fraud risks, conflicts of interest and irregularities involving ESI Funds. Data sources for Arachne include data from MAs as well as external databases (e.g. ORBIS and World Compliance). In December 2018, according to the EC, 21 Member States used Arachne for 165 OPs, which accounted for 54% of all EU cohesion funding for 2014-20 (excluding the European Territorial Co-operation objective of the European Regional Development Fund) (European Court of Auditors, 2019[4]). See Box 2.2 for more details on the risk data Arachne makes available.

Box 2.2. Arachne risk categories, indicators and overall risk score

Arachne can display 102 individual risk indicators. Each indicator has its own calculation rule that can be displayed in a pop-up window. Arachne can only display a risk indicator if all data for its calculation are sent by the MA. All of them are grouped into the 7 risk categories of procurement, contract management, eligibility, performance, concentration, reasonability and reputational and fraud alerts. The number of risk indicators in each risk category varies. Whereas the procurement category has 6 risk indicators, the reputational and fraud alerts category has 30.

The maximum score of an individual risk varies between 5 and 20, depending on the type of risk. A score of 0 means that Arachne did not detect any risk for that specific indicator. A maximum score (5, 10, 15 or 20) means that Arachne identified a potential risk. A general score is also calculated for each category (with 50 the maximum). Arachne enables the managing authority to easily identify the riskiest projects, contracts, contractors and beneficiaries with the help of the "overall risk" score, which is the average of the seven risk categories.

Arachne supports analysis of different types of fraud risks and red flags, including the following:

- *financial* – the overall financial performance of beneficiaries, contractors/suppliers and subcontractors, based on financial reporting data
- *relationship* – the existence of relationships between beneficiaries and contractors/suppliers or subcontractors and their respective personnel
- *reputation* – involvement in activities (such as bankruptcies) that could possibly result in reputational damages
- *sanctions* – identification of beneficiaries, contractors/suppliers, subcontractors or their respective personnel blacklisted by appearing in any type of sanctions list
- *change* – any type of changes to the company structure
- *procurement* – the lead time between publication of the tender notice and contract signature
- *contract management* – contract addenda cost (total) for the project and actual project cost
- *eligibility* – project costs outside the eligibility period, such as before the start date or after the end date
- *performance* – number of people trained or to be trained
- *concentration* – beneficiaries involved in multiple projects
- *other checks* – EC financial assistance and total project cost

Source: (OECD, 2017[20]) and (European Commission, 2017[21]).

In the Slovak Republic, MAs have actively used this tool since late 2018, and its use is in fact mandated in a methodological note for Arachne prepared by the CCB. MAs supplement Arachne with several other databases, including the ITMS 2014+, IMS, the Early Detection and Exclusion System, company registers and procurement databases. MAs said that the most commonly applied data analytics techniques they use with the support of these systems are traditional rules-based detection and descriptive tests, such as data matching and data mining. Data from ITMS 2014+ are transferred to Arachne and updated every two weeks.

The OECD identified one main area for MAs to improve the use of Arachne for assessing integrity risks. Based on workshops and discussions with MAs, officials said the MAs lacked experience in using Arachne and reported difficulties in interpreting its outputs, which include a multitude of reports and dashboards.

During the OECD mission, MAs emphasised the need for more guidance and training on the use of Arachne for detecting, preventing and managing fraud and corruption risks in ESI Funds. Guidance is not completely lacking: for instance, in 2018 the aforementioned methodological note from the CCB explains the baseline functionalities and application of Arachne. However, the note provides limited guidance to support the MAs in the practical use of Arachne to assess risks. Ineffective or inefficient use of Arachne can produce an administrative burden and undermine its adoption and benefits. Additional guidance and training could help to address the knowledge and skill gaps, going beyond functionalities.

Key Action: Further define objectives and expand the use of Arachne for assessing risks within MAs, with practical guidance from the CCB

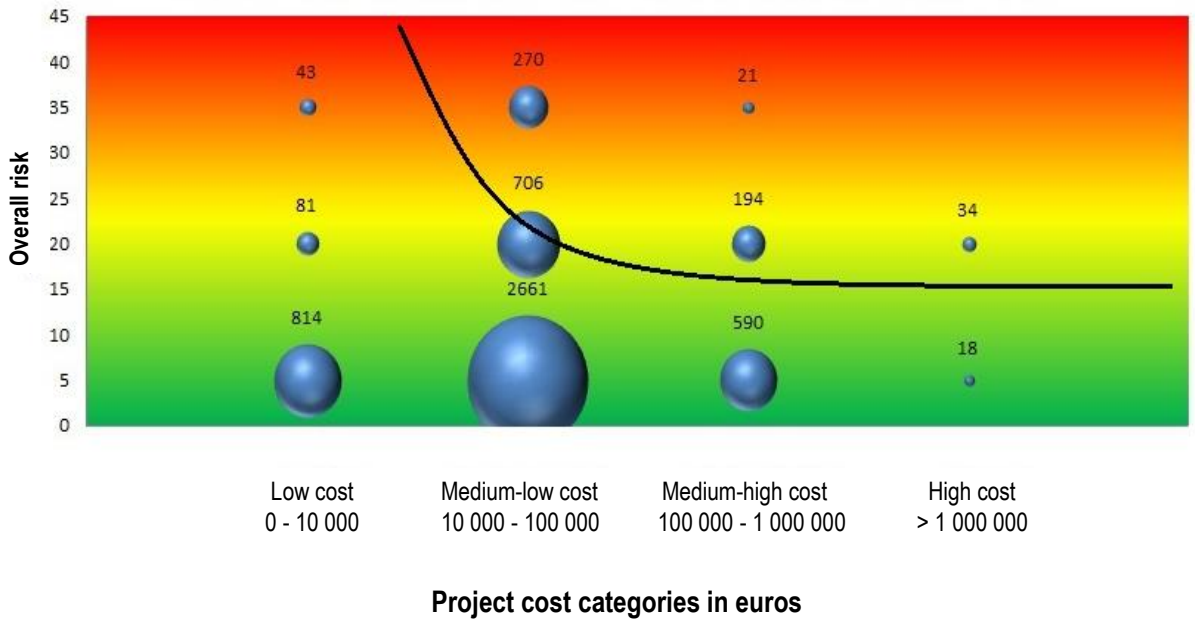
Users primarily employ Arachne to assess conflicts of interests and analyse fraud across different processes, sectors and OPs (PWC, 2018[17]). Nonetheless, Arachne has additional potential as a tool for MAs to assess risks. On an aggregated level, Arachne can display historical evaluation and risk trends of an OP to inform risk assessments. EC reports show, for example, that Arachne can furnish statistical analysis and data about the distribution of projects and project costs among risk categories. Moreover, Arachne allows for analysis of the correlation among several factors, including project cost, region, and individual risk scores, and can thus shed light on hidden fraud patterns.

These different types of analyses that Arachne can support underscore the need to set objectives when using it, as is the case with any data analytics tool or technique. One objective for the assessment could be to identify integrity risks in individual project (or among specific) contractors or beneficiaries. However, there are other questions that could shape or complement this objective and therefore lead to different types of analyses. To improve on the existing methodological note, the CCB – with input from the MAs, the Anti-Corruption Unit of the government office and other key stakeholders – can provide additional guidance and training for the effective use of Arachne, with a focus on helping MAs to set objectives as well as practical considerations for assessing integrity risks. This can also include elaboration on the full capabilities of the Arachne tool, such as strategic analysis and management verifications (including administrative and on-the-spot verifications). Pursuant to EU Commons Provision Regulation No. 1303/2013, MAs should include administrative verifications (i.e. a desk review) of each application by beneficiaries for reimbursement as well as on-the-spot checks of operations (European Commission, 2015[22]).

Systemic analysis

MAs in the Slovak Republic indicated they do not perform a systemic analysis of their respective OPs. Upon request from a Member State, the EC can provide a report with programme analysis of data from each OP, which includes an aggregate review for each risk category as well as the overall risk score for all projects (as described in Box 2.2). This use of Arachne can provide an overall picture of risk, and help MAs target further risk analysis and controls. For example, Figure 2.3 shows the distribution of projects for an OP in the Slovak Republic by project cost category and overall risk score for the 2007-13 ESI Fund programming period. It suggests, perhaps counter-intuitively, that costs alone do not provide a strong indication of risk, as the projects with the highest costs have lower overall risk scores than those categorised as low-medium cost (i.e. in the cost range of EUR 10 000 to EUR 100 000).

Figure 2.3. Number of projects per project cost category and overall risk score



Note: The figure presents the European Social Fund's 2007-13 project distribution.
Source: Statistical analysis generated by the EC for the Slovak Republic using the Arachne system.

The report can also provide insights on fraud, reputational, and concentration risk indicators. The latter shows whether a project partner or contractor is involved in more than one programme or project. High levels of aggregated and individual scores in these categories can be a key signal for MAs to focus their attention on them when carrying out control activities.

Data-driven administrative verifications

Overall risk scores offer a useful but incomplete picture of the risks in ESI Funds; MAs should therefore be cautious about relying solely on that score. Indeed, discussions with MAs indicated that they pay the most attention to overall risk scores and that the threshold they follow is their maximum level (i.e. 20, as described in Box 2.2). Strict adherence to this score and threshold could lead the MAs to overlook other issues. For instance, projects with acceptable overall scores can present high risks in specific risk categories (i.e. procurement, reputation, fraud alerts and concentration). Guidance for MAs should support analysis of individual risk categories at the operational level, with a focus on helping MAs identify patterns, root causes and linkages among risks. This analysis can support the process of verifying claims for reimbursements, and ensure that any detected irregularities during verification are excluded from expenditures declared to the EC.

Data-driven on-the-spot (OTS) checks

MAs are required to undertake OTS checks of operations. When conducting these checks, the EC requires quantitative and qualitative assessments of any irregularities detected in order for the MA to understand the prevalence and severity of risks in other operations that it did not sample. The MA should then take corrective measures (European Commission, 2015[22]). In the Slovak Republic, MAs could make better use of Arachne to support these activities. Discussions with MAs suggested that OTS checks largely focus on conflict of interest and the operations that are checked are decided arbitrarily, with limited consideration of risk data or where the highest risks may lie. Using Arachne for the preparation of OTS checks can allow

better targeting of activities as well as more effective and efficient use of resources. For instance, Arachne can help MAs understand whether improper links exist between the beneficiary and contractors, and it can highlight historical trends to elucidate how risks evolve over time as well as fluctuations in risk scores. The OECD also identified one example where a contract was agreed with companies that were barred from being involved with ESI-funded project implementation, which should have triggered questions about the selection process and potentially false statements submitted by the contractor. Arachne can also provide information to MAs about whether beneficiaries own companies with residences in tax havens or have high-risk scores in key categories like procurement. Practical guidance from the CCB and training for MAs can improve identification of such risks and other red flags, drawing on the available data in Arachne. Building knowledge and skills in this area will also rely on close co-operation with organisations from the AFCOS network, including investigation units, Public Procurement Office and police/law enforcement bodies. That co-operation will be vital, as discussed further in Chapter 3.

Proposals for Action

Towards enhancing fraud and corruption risk assessments

Action	Description	Entity/entities with primary responsibility	Time frame (short, medium, long term)
1	Review and update risk assessment procedures to ensure greater clarity for identifying fraud and corruption risks across the ESI Funds project cycle	MAs/risk management working groups or risk management functions within MAs	Short
2	Clarify and improve the criteria for scoring fraud and corruption risks	MAs/risk management working groups or risk management functions within MAs	Short
3	Ensure control activities are appropriate, sufficient and proportional to identified risks	MAs/risk management working groups or risk management functions within MAs	Short
4	Develop a plan for more effective use of data on irregularities and public procurement	MAs/CCB	Long
5	Conduct periodic statistical analysis of irregularities, fraud cases and audit findings to help determine higher-risk areas in different sectors across the whole system	CCP OLAF/MAs	Medium
6	Further define objectives and expand the use of Arachne for assessing risks within MAs, with practical guidance from the CCB	MAs/CCB	Medium

Notes

[1] There are a variety of methods and tools for exploring root causes of risks and conducting cause-effect analysis, the details of which are beyond the scope of this discussion. For instance, when identifying risks or analysing the external and internal context, MAs could explore the use of Iskhikawa or "fishbone" diagrams, decision trees, process and influence maps or methods of assessing context, such as the "PESTLE" method (Political, Economic, Social, Technological, Legal and Environmental).

[2] Procurement provisions for ESI-funded projects follow EU directives and national legislation.

3 Adopting a systematic approach to managing fraud and corruption risks in European Structural and Investment Funds in the Slovak Republic

Introduction

A truly systematic approach, whereby risk management is undertaken routinely and integrated into existing processes, is vital for effective fraud and corruption risk governance within the public sector. Fraud risk governance not only relates to systems and policies; it also shapes the culture of an organisation, and its capacity and readiness to deal with risks. By endorsing anti-fraud policies, senior management can demonstrate its commitment to a culture of integrity, and lay out provisions for the fraud risk management process. Managing authorities (MAs) in the Slovak Republic have developed and adapted their procedures regarding fraud risk assessment in line with the European Commission's *Guidance Note on Fraud Risk Assessment and Effective and Proportionate Anti-Fraud Measures,* developed by the Expert Group on European Structural and Investment Funds (hereafter EGESIF) (European Commission, 2014[14]). However, MAs could further integrate fraud risk management activities into existing practices. This includes developing stand-alone anti-fraud policies and fostering a proactive risk culture. In addition, MAs could take steps to build skills and invest in the training needed for improving the capacity of employees to carry out assessments that account for fraud and corruption risks. Improving capacity can further expand and anchor good practices.

In addition, enhanced co-operation and knowledge sharing are vital to ensure that programme authorities are maximising their skills and expertise to mitigate fraud and corruption risks. In the Slovak Republic, MAs do not regularly involve other authorities responsible for ESI Funds management or oversight. Nor do they communicate effectively with law enforcement authorities such as the General Prosecutor's Office (GPO) once cases of fraud or corruption have been referred to those bodies. By establishing a task force within the Anti-Fraud Co-ordination Service (AFCOS) network, the Government of the Slovak Republic can provide MAs with the means to improve their risk assessments, and ensure that fraud and corruption risk management is embedded in authorities' practices. Furthermore, setting up information-sharing forums between programme authorities and law enforcement authorities can keep MAs up to date regarding evolving fraud and corruption activities, which can then be used in future risk assessments.

Another key area for effective governance of risk management is monitoring and evaluation (M&E). International standards emphasise the need for governments to perform M&E in order to assess outcomes and update activities to improve fraud and corruption risk management (COSO, 2016[16]). Moreover, the European Commission (EC) encourages Member States and programme authorities to define procedures for monitoring the implementation of fraud prevention and detection measures. This includes reporting what anti-fraud measures have been set up, and how effectively they have been applied. In this context, the unit of analysis for M&E is not individual risks, but the entire system in place for managing them. Specifically, M&E involves the systematic collection of evidence dealing with the design, implementation and results of the policies, controls and actions taken to manage fraud and corruption risks. Effective monitoring allows managers to adapt when issues arise while evaluations offer insights into an ongoing or completed activity, to support decisions about relevance, effectiveness and potential alternatives.

M&E is not the sole responsibility of audit entities or other oversight bodies. Responsibility for monitoring and evaluating fraud risk management is a shared one that concerns MAs, the Audit Authority (AA), and working groups. M&E can moreover act as a management tool to drive improvements in specific areas, such as the governance structure for risk management and risk assessments, by integrating lessons learned and feedback loops. In discussing paths to better governance for managing risks, this chapter also explores ways that MAs can refine their approaches to evaluating risk management activities, particularly fraud and corruption risks, and in so doing continuously improve risk management involving ESI Funds.

Taking into account these governance issues, this chapter focuses on the following priorities:

- Priority 1: Develop explicit anti-fraud policies and foster a positive risk culture
- Priority 2: Establish a formal mechanism for co-ordination among authorities
- Priority 3: Increase the capacity to manage fraud and corruption risks with improved training
- Priority 4: Improve feedback loops with law enforcement authorities to enhance risk assessments
- Priority 5: Monitor and evaluate fraud risk management activities and controls

Priority 1 – Develop explicit anti-fraud policies and foster a positive risk culture

Issue analysis

Legal and policy frameworks in the Slovak Republic provide the foundation for fraud risk management relating to the implementation of ESI Funds, such as the government's National Anti-Fraud Strategy (NAFS) and the methodological setting of risk management practices by the Ministry of Finance. Moreover, the EC provides programme authorities with guidance on developing anti-fraud policies as part of their strategic anti-fraud measures, such as working to promote an anti-fraud culture and allocating responsibilities for tackling fraud. As of 2019, the four MAs participating in the OECD project had developed such policies; some had been approved while others were in the process of being approved by the Secretary-General of the relevant ministry. However, the OECD identified several MAs in the Slovak Republic that have yet to fully adopt anti-fraud policies relating specifically to ESI Funds – even if, in general, MAs have established risk management procedures to implement operational programmes (OPs),

Risk management is a growing practice across the Slovak public sector. Anti-fraud policies serve as a valuable tool to embed fraud and corruption risk management into MA practices, and ensure that risk management is sustainable. Some MAs currently have anti-fraud policies in place that include an explicit statement on corruption and fraud risk management responsibilities and activities; it is vital that the remaining MAs establish such policies. Besides ensuring that employees are aware of their fraud risk management obligations and promoting a positive risk culture within MAs, these policies can also communicate to other stakeholders – including the public – that MAs are committed to mitigating fraud and

corruption risks in the implementation of OPs. Regarding the participating MAs, only one has made their anti-fraud policy available on line.

In addition, managing fraud and corruption risks in the Slovak Republic is heavily focused on compliance. As a result of the compliance-based approach used by MAs to examine fraud and corruption, certain risks may not be given adequate attention and may not be properly prioritised. Moreover, some MAs have risk management procedures that do not include explicit mention of managing fraud and corruption risks. According to systems audits undertaken in 2017, these are analysed with other types of risks included in risk assessments. In the case of one OP, the AA concluded that the MA did not sufficiently identify fraud risks in the Catalogue of Selected Risks, implying that the MA did not determine that this category of risk merited attention.

Key action: Have managing authorities develop and approve a tailored anti-fraud policy and disseminate it widely

Senior management in the MAs that do not currently have an anti-fraud policy can establish one tailored to their OPs. The policy can demonstrate senior management expectations, their commitment to integrity, and a zero-tolerance approach regarding fraud and corruption. The policy may vary depending on the context of different MAs and the maturity of their risk management function, but it should achieve the following:

- *Articulate the anti-fraud and anti-corruption objectives of MAs in implementing OPs* – An explicit policy is a communication tool for MAs and employees involved in implementing ESI-funded projects. The policy should include definitions of fraud, corruption and irregularities, and make explicit linkages between the anti-corruption and anti-fraud objectives of MAs and their risk management activities. These objectives should be considered alongside those of the OP, taking into account the types of fraud and corruption that pose the highest risk in this context.
- *Clearly define roles and responsibilities regarding fraud and corruption risk management* – MAs are responsible for identifying and managing risks, but successful fraud risk management depends on the contribution of each employee within the MA. Alongside their risk management functions, managers within MAs are responsible for the day-to-day handling of fraud and corruption risks. Their tasks include ensuring that internal controls are in place and functioning, and (more generally) preventing and detecting fraud and corruption risks. These different roles should be outlined in policy.
- *Detail the steps involved in fraud reporting and investigation procedures* – Employees within MAs should be aware of the appropriate channels to use when reporting suspected fraud or corruption. This would include clearly detailing how staff report internally and to external bodies (i.e. law enforcement authorities, and the European Anti-Fraud Office [OLAF]), and the actions that should be triggered when potential fraud or corruption is reported.
- *Stipulate how the fraud risk management framework should be monitored* – Policy should detail how fraud risk management activities will be monitored and evaluated, for example through periodic or ongoing evaluations, and also outline who is responsible for undertaking these activities (The Chartered Institute of Public Finance & Accountancy, 2014[23]; COSO, 2016[16]). Later in the chapter there are further examples of and discussion about monitoring and evaluating risk management activities.

For those MAs that do not currently have an anti-fraud policy in place or are in the process of developing one, opportunities remain to design policies that go beyond alignment with EGESIF. Given that fraud and corruption risks differ among OPs and among MAs, these policies should not be one-size-fits-all: different entities have different objectives and varied risk profiles (GAO, 2015[19]). Anti-fraud policies should take into account the fraud risk scenarios encountered by the MA in question. An anti-fraud policy in fact provides an opportunity to define fraud and other types of misconduct. A European Court of Auditors report

from 2019 found that not all Member States interpret the European Union (EU) definition of fraud in the same way, meaning that some fraudulent activities are not reported by programme authorities (European Court of Auditors, 2019[4]). MAs in the Slovak Republic should ensure that the anti-fraud policy provides clear definitions of what constitutes fraudulent or corrupt activity, in line with EC definitions. Box 3.1 provides an example of a comprehensive counter fraud policy for the European Regional and Development Fund in the United Kingdom.

Box 3.1. A comprehensive Counter Fraud Policy for the European Regional Development Fund in the United Kingdom

The UK *Counter Fraud and Conflict of Interest Policy for the European Regional Development Fund 2014-2020 Programme* is updated regularly and contains detailed provisions on the following:

- senior management responsibilities regarding fraud and corruption in the fund
- internal and external communication
- the Counter Fraud Team's responsibilities, as well as those of other staff
- fraud detection methods (internal and external)
- fraud investigation and sanctions
- updates on the use of the European Commission's Arachne tool for risk scoring
- the fraud referral process and reporting details
- the scope of the conflict of interest policy, including updating of that policy.

The policy applies to all staff working on implementation of the fund's operational programmes, including partners, grant recipients, final beneficiaries and other stakeholders. The strategy sets out the managing authority's commitment to preventing, detecting and deterring fraud and corruption, and to taking action where fraud or corruption is suspected or detected. The strategy centres on four key themes: prevention, detection, investigation and sanction.

It aims to ensure that the European Regional Development Fund 2014-20 Programme is protected against fraud and loss; embed an "anti-fraud" culture that mainstreams commitment to zero tolerance to fraud and sets out the roles and responsibilities of all staff in ensuring achievement of this objective; actively encourage detection by putting in place checks at different stages of business processes to act as a deterrent to fraudulent and corrupt acts; provide a clear route map for investigation and remedial action; and provide clear guidance for identifying, declaring and recording conflicts of interest. Once updated, the policy explicitly states which provisions have been amended.

Source: Developed from interviews in the course of the OECD mission, February 2019.

For the MAs that already have an anti-fraud policy in place, a review of the policy could allow for further improvement of its components. For instance, an annual review could be undertaken by senior management to assess its relevance in relation to the fraud risk profile of the MA. Inputs from previous risk assessments, fraud reporting, results of investigations and audit reports can be used during the review process. In line with this strategy, updated anti-fraud policies could include information on how the MA is using data-driven approaches to mitigate fraud and corruption risks, as well as outlining the measurement criteria and tools that will be used to evaluate their fraud risk management activities (see Priorities 5 and 6). Once established, updated and approved, the anti-fraud policy of each MA should be visible both within the entity and externally. This can include publishing the policy on the intranet and distributing it to staff members. To ensure that the public and third parties involved in the implementation of OPs can see the

commitment of MAs to combating fraud and corruption, the policy can also be published on line via the webpage of the responsible MA or the OP webpage.

Priority 2 – Establish a formal mechanism for co-ordination among authorities

Issue analysis

When conducting risk assessments, MAs expressed a need for improved co-ordination. Nonetheless, none of the MAs involves other authorities responsible for ESI Fund management or oversight, such as the certifying authority (CA), intermediate bodies (IBs), the Anti-Fraud Co-ordination Service (AFCOS), audit authority (AA), Corruption Prevention Office (CPO) and Public Procurement Office (PPO) in the risk assessment process. The limited co-operation that exists among these authorities is centred on policy co-ordination and high-level information sharing, but co-ordination is not focused on fraud or corruption risk management directly. The absence of inputs from these stakeholders may lead to incomplete risk assessments, because identification and analysis could overlook certain risks recognised by other authorities. For instance, the CA can have a more comprehensive view of fraud risks concerning certification and payments. AFCOS can bring specific anti-fraud expertise and knowledge of new and evolving schemes into the assessment process. The PPO collects data on breaches and infringements of procurement processes in OPs, which may reveal high-risk areas during this stage. The CPO provides a comprehensive list of potential corruption risks for various sectors that may inform risk assessments.

A core element of effective risk management is communication, which means the timely involvement of stakeholders to take into consideration their knowledge, views, and perceptions. This risk management principle implies a systematic approach to communication and consultation, sharing information with targeted audiences, and obtaining feedback from relevant parties to shape risk management (ISO, 2018[24]). Several EU Member States, such as the Netherlands and Spain, have transitioned to a more co-operative approach to conducting fraud risk assessments. In doing so, they bring together diverse expertise and insights regarding anti-fraud and anti-corruption measures. Such an approach has allowed these Member States to establish risk-based measures for managing fraud risks more effectively (PWC, 2018[17]). In France, the General Commission for Equal Territories (CGET) has organised regular meetings for all the authorities responsible for European programmes covering different topics, including the fight against fraud (Box 3.2).

Box 3.2. Inter-departmental co-ordination in the fight against fraud involving European Structural and Investment Funds (ESIF), France

In France, the General Commission for Equal Territories (CGET) co-ordinates authorities so as to facilitate and safeguard implementation of programmes co-financed by ESIF. In 2013, the CGET set up an inter-fund working group on the subject of fraud in direct response to requests by the authorities responsible for European programmes. It has since also drawn up reference documents.

In the context of its fortnightly meetings with the directors in charge of implementing operational programmes, the CGET has invited a representative of the National Anti-Fraud Unit, the French Anti-Fraud Subcommittee and AFCOS to come and outline the Commission's expectations concerning the fight against fraud involving structural funds. The tools developed by OLAF and the National Anti-Fraud Unit for detecting fraud in connection with ESIF are available on the CGET digital platform, bringing together all actors involved in implementing ESIF in France. Finally, the national technical assistance programme 2014-2020 plans to fund training courses for OP managing authorities, Certifying Authorities and Audit Authorities in different areas, including anti-fraud measures and public procurement.

Source: (European Commission, 2017[25]), "Follow-up of recommendations to the Commission report on the protection of the EU's financial interests: Fight against fraud, 2015", https://ec.europa.eu/anti-fraud/sites/antifraud/files/2_autre_document_travail_service_part1_v2_en.pdf.

In addition, the AA can offer insights based on its audits while continuing to maintain its independence as an audit institution. The EC provides guidance to Member States on a common methodology for assessing Management and Control Systems (MCS), including assessment criteria for Key Requirement (KR) 7 on anti-fraud measures (European Commission, 2014[26]). Under Regulation No. 1303/2013 of the Common Provisions Regulation (CPR) (European Parliament, 2013[27]), the AA is required to carry out systems audits of the MCS of MAs, IBs, and CAs. Systems audits aim to obtain reasonable assurance that MCS function effectively and efficiently to prevent errors and irregularities (including fraud) and that, if these appear, the system is capable of detecting and correcting them. In the Slovak Republic, the AA performs system audits of the completed risk assessments per KR 7 on anti-fraud measures, and therefore may need to limit its role in designing the risk assessments for MAs. Nonetheless, the AA can participate in an advisory capacity, as it will have a government-wide vantage point from which to inform the identification of risks and honing of risk assessments.

In interviews with the OECD, MAs highlighted different expectations they have with regard to the anti-fraud measures they should be implementing and the criteria by which the AA audits their MCS. Specifically, the AA adheres strictly to EGESIF guidance, whereas some MAs view that guidance as a starting point and aim to tailor their practices to specific contexts. Such strict adherence can result in missed opportunities for MAs to properly adapt their risk management activities and use the resulting audits to improve fraud and corruption risk management practices.

The first step in addressing these issues is to improve communication among stakeholders and encourage engagement with the AA. Constructive and frequent communication between the AA and MAs can help improve the overall resilience of ESI Funds to fraud and corruption while allowing the AA to remain independent. See Box 3.3 for an example of how the AA in the Netherlands works with programme authorities to improve fraud prevention and detection, and sets the expectation for audits. In other Member States such as Estonia, Ireland and Lithuania, the AAs play a role in fraud prevention through advising MAs and CAs. For example, the Irish AA has created a list of fraudulent practices detected during their audits to spread fraud awareness to the relevant authorities. To further enhance fraud and corruption risk

management, more frequent exchanges between MAs and the AA would be particularly beneficial as part of the M&E processes. Allowing such exchange would provide structure, incentives and shared objectives, so that communication among AAs, MAs and others go beyond ad hoc activity and towards a more systematic approach.

Box 3.3. A multi-stakeholder approach to enhancing the role of auditors in fraud and corruption prevention involving ESI Funds: The Netherlands experience

In the Netherlands, the audit authority (AA) has adopted a "trust but verify" approach to its duties in the ESI Funds context. While the AA recommends that managing authorities (MAs), intermediate bodies (IBs) and the certifying authority (CA) use the guidance note for assessing key requirements (KR) at the systems level as a self-assessment tool, it recognises that this should be tailored to the specific management and control systems of each authority. In practice, this means that the AA provides a degree of flexibility in its approach.

Utilising its knowledge and experience from the previous programming period, the Netherlands AA assisted in the setup and use of the self-assessment tool, which has better prepared the programme authorities for systems audits. In addition, the AA provided training and capacity-building activities to develop expertise in the area of fraud prevention and detection within programme authorities. The AA is included in a monthly roundtable meeting with MAs and the CA, which provides a space for the different authorities to discuss challenges arising from audits of the respective management and control systems. There are also technical meetings that take place twice a year, organised by one authority. These meetings enable the exchange of knowledge and expertise and allow the AA to provide input regarding the functioning of programme authorities' management and control systems.

Source: Developed from interviews in the course of the OECD mission, February 2019.

Key Action: Create a task force in the AFCOS network to enable knowledge sharing and exchange of good practices between managing authorities and key stakeholders

MAs could benefit from improved interactions and sharing of experiences, particularly with regard to practices for managing and assessing risks. In workshops organised by the OECD, the participating MAs voiced a strong desire for a knowledge-sharing platform dealing specifically with the issue of combating fraud and corruption in ESI Funds. Regular exchanges on fraud and corruption risk assessments can help enhance individual OP risk assessments and improve coherence across programme authorities, all the while recognising the need for tailoring to different contexts. In addition, MAs could work together to strengthen their fraud risk assessments by inviting a wider range of authorities to exchange views on and experiences with potential fraud risks and appropriate mitigating actions.

In the Slovak Republic, a key co-ordinating body in the anti-fraud and control architecture is the Central Contact Point (CCP) OLAF, which performs the role of the Anti-Fraud Co-ordination Service (AFCOS) that exists in each EU Member State. The AFCOS network consists of bodies involved in the management and implementation of ESI Funds, notably MAs, IBs, the CA and AA, and numerous other authorities such as the PPO, the Supreme Audit Office of the Slovak Republic (NKU), the Anti-Monopoly Office (AMO), GPO, and the Ministry of Justice. The Steering Committee for the Protection of the Financial Interests of the EU, which is made up of representatives from different programme authorities, co-ordinates and supports co-operation among AFCOS network partners. Before the updated National Strategy for the Protection of the European Union's Financial Interests was approved on 30 May 2019, there were five working groups under the steering committee. The working groups held periodic meetings on the following topics: irregularities,

Article 325 of the Treaty on the Functioning of the European Union (TFEU), co-operation in the co-ordination of control activities, public procurement, and communication.

The existing structure could accommodate a platform for co-ordination and knowledge sharing among MAs, IBs, the AA, and the CA on issues relating to fraud risk management in the implementation of ESI Funds. Formal co-ordination can take the form of a task force with resources and expertise in fraud and corruption risk management. MAs can ensure that experienced and well-informed representatives participate on this task force. Programme authorities could also organise frequent and regular meetings or workshops with MAs, IBs, the CA and AA, and other AFCOS network partners to share good practices for managing fraud and corruption risks. Specifically, representatives from the respective risk management working groups can establish regular interactions to develop more comprehensive approaches to conducting fraud risk assessments. Workshops and discussions can be facilitated by experts, both internal and external, that possess experience in managing fraud and corruption risks involving ESI Funds. With assistance from CCP OLAF, the task force could invite other authorities, including the CPO, PPO and NKU to provide input in discussions on improving fraud and corruption risk assessments. The Central Co-ordination Body (CCB) can also support the task force in facilitating co-operation.

Priority 3 – Increase the capacity to manage fraud and corruption risks with improved training

Issue analysis

Based on the OECD review of relevant documentation and interviews with practitioners, the current risk management practices of programme authorities in the Slovak Republic reveal a lack of capacity in identifying and analysing fraud and corruption risks (see Chapter 2). MAs in many EU Member States share the same challenge: they are expected to implement ESI-funded projects in compliance with numerous legal provisions set out by the EC, while also developing effective anti-fraud measures (a central theme during the current programming period). As a result, Member States may not have developed sufficient expertise or skills relating to the implementation and monitoring of anti-fraud measures or performing risk assessments. In the Slovak Republic, MAs could build expertise in fraud risk management by developing and planning anti-fraud training tailored to the specific context of each OP.

As of 2019, several MAs in the Slovak Republic are handing anti-fraud training over entirely to external bodies such as CCP OLAF. That office has organised training activities and seminars for AFCOS network partners based on the Training Plan for the Protection of the EU's Financial Interests in the Slovak Republic. The list of training programmes for 2017-18 shows that ten seminars took place covering a wide variety of topics: building awareness of fraud; the most common infringements of public procurement rules; detection of fraudulent practices in the implementation of ESI Funds; and cartels and distortion of competition. One seminar in 2017 focused on risk management and the set-up of control mechanisms in structural funds. Another training session dealing with management of fraud and corruption risks involving ESI Funds is planned for 2019. The number and nature of trainings organised by CCP OLAF depend on the available budget and needs of the AFCOS network partners. As such, trainings may be ad hoc and irregular.

Overall, representatives from the risk management working groups see opportunities for receiving more specific and practical training in identification, analysis and management of fraud and corruption risks in structural funding. Moreover, Member States are required by the EC to provide training for staff involved in verifying the use of ESI Funds specifically concerning potential fraud, sharing information on detected fraud cases, red flags, and practical application of available tools. The Slovak Republic Government's own National Anti-Fraud Strategy stipulates that all employees involved in implementing ESI Funds should receive integrity training, as well as technical training to help them better identify and analyse risks.

Explicitly, the NAFS states that training should focus on strengthening the skills of employees to recognise red flags and cases of suspected fraud, and the steps to take in response. In addition to capacity building, training staff on specific anti-fraud measures helps raise awareness of the commitment of MAs to fighting fraud and corruption involving structural funds (European Commission, 2014[14]).

Key action: Develop formalised, regular, and ongoing training programmes on fraud risk management and assessments for personnel in managing authorities

CCP OLAF and MAs can establish formalised, regular and ongoing training programmes to complement ad hoc seminars for developing skills in fraud and corruption risk management. Since training resources are limited, training priorities should primarily target staff with direct responsibility for identifying, analysing and mitigating fraud and corruption risks. These employees can include participants from risk management working groups and personnel within MAs and IBs who carry out control activities such as on-the-spot (OTS) checks, internal audits and investigations. Trainers can use employee surveys, international recommendations and consultation groups to identify training needs. In addition, regular training assessments can help ensure that staff trainings within MAs and IBs take into consideration the particular fraud and corruption risks associated with the OPs that they are implementing. Based on the OECD review of the needs and challenges of MAs, key topics to consider include:

- fraud and corruption risk identification and analysis
- indicators and red flags for potential fraud and corruption
- practical co-operation and information exchange between law enforcement agencies and programme authorities – for example, sharing information on cases, best practices and recommendations made
- monitoring and oversight of contractors and subcontractors
- components of an internal control system and risk management practices in public institutions
- administrative investigation of tips received from whistleblowers and other reporting channels.

Another way to formalise training is through professional certification. MAs can facilitate training and skills acquisition by encouraging employees to attain internationally recognised qualifications, such as the Institute of Internal Auditor's Certification in Risk Management Assurance, the Association of Certified Fraud Examiner's certification, or the Certificate in Fraud Risk Management from the Chartered Institute of Public Finance & Accountancy. Furthermore, training programmes should be holistic in nature and include guidance not only on fraud risk management, but also on how to foster a culture of integrity. Interactive activities can be employed as training techniques, such as dilemma training whereby employees are presented with particular situations and ways to deal with them realistically. Such exercises may be more effective at instilling knowledge than formalistic check-the-box activities. Experiential learning activities can prepare employees who undertake risk assessments and populate risk registers, as demonstrated in the example from the Netherlands (Box 3.4).

Box 3.4. Practical anti-fraud training in Poland and the Netherlands

An e-learning platform on fraud and corruption in Poland

In 2014 the Central Anti-Corruption Bureau (CBA) in Poland developed a free e-learning platform with financial support from the European Commission. The goal of this platform, which evolved from an on-site anti-fraud training programme for public officials, is to raise participants' awareness of corruption and fraud in public administrations and companies, as well as raising public awareness of anti-corruption efforts. Between May 2014 and November 2017, 46 626 people took the training course; November 2017 saw 61 272 participants; and there are currently 126 757 enrolees, 25 017 of whom completed the course on corruption in public administration since the new platform was launched. The sheer number of participants and its growing prevalence demonstrates the impact it has had on public sector entities.

Incorporating anti-fraud games into training activities in the Netherlands

Following detection of several cases of fraud and misuse of ESI Funds in the programming period 2007-13, authorities in the Netherlands acknowledged the need to strengthen the anti-fraud capacity of managing authorities (MAs), intermediate bodies (IBs), the certifying authority (CA) and the audit authority (AA). This led to the Dutch Ministry of Finance developing an anti-fraud game within a broader anti-fraud training programme. The anti-fraud game is highly interactive and makes use of several multimedia tools such as video and animations to retain the attention of participants during the session and foster a rapid learning process by associating a concept or information taught with a sound, image, video or object. The aim is neither to provide a traditional training course covering EU laws and regulations, nor to provide a set of ready-to-use anti-fraud measures for integration into their management and control system procedures. Instead, the anti-fraud game training was invented to motivate and encourage participants – as well as develop their ability – to identify red flags of fraud and corruption by being more aware, attentive and responsive to hints and cues of fraud. This more readily allows them to put in place the most appropriate and effective anti-fraud control measures.

The anti-fraud game is intended for the extensive group of ESI Funds stakeholders, including MAs, IBs, the CA and the AA from all EU Member States and EU candidate countries, and more general practitioners working with EU and national funds. However, it can easily be adapted to a single stakeholder group or a mix thereof. A game session includes a maximum of 35 to 40 participants.

Source: The example from Poland is gathered from the Senior Party of Integrity Officials that took place in November 2019. Additional references can be found at https://szkolenia-antykorupcyjne.edu.pl/. The anti-fraud training game from the Netherlands was delivered by an expert during an OECD mission to the Slovak Republic in February 2019.

Introducing immersion seminars and peer-to-peer exchanges can also enhance training activities and strengthen participants' capacity to manage fraud and corruption risks involving ESI Funds. To increase training resources and expertise so as to share good practices and deliver capacity-building workshops, relevant authorities such as CCP OLAF, MAs, CAs and the CCB could seek support from experts and skilled practitioners from other EU Member States. Two specific programmes that allow such exchange and capacity building are TAIEX-REGIO Peer 2 Peer and Hercules III. TAIEX is designed to enable public officials managing the European Regional Development Fund and Cohesion Fund to exchange knowledge and find realistic solutions to problems. Three types of technical assistance are expert missions, study visits and workshops, which are financed by the EC. Hercules III helps to fund projects including training activities, which can help combat fraud and corruption. This programme provides opportunities for experts to share best practices through seminars and conferences on a variety of topics such as corruption prevention in procurement. It can also cover more specialised training to improve skills in digital forensic detection and fraud prevention.

Capacity building requires ongoing investment and resource allocation, which appears to be a major constraint in the Slovak Republic. When developing plans for the next programming period (2021-27), the CCB and MAs could establish a dedicated budget in the national technical assistance programme to fund training courses related to fraud and corruption risk management and anti-fraud measures. The objectives of training programmes should meet the requirements of the NAFS and the priorities of the government of the Slovak Republic in reducing fraud and corruption risks. Risk management procedures for some OPs utilise fraud indicators, but this practice has not yet been implemented in all MAs (see Chapter 2). For example, the internal documentation of OP Quality of Environment provides a comprehensive list of red flags, particularly those that are relevant in the procurement cycle. Other MAs can further develop and expand training in this area to ensure that staff in MAs are aware of fraud indicators and red flags and so can respond proportionately to potential fraud and corruption.

Priority 4 – Improve feedback loops with law enforcement authorities to enhance risk assessments

Issue analysis

Throughout the implementation of OPs in the Slovak Republic, co-ordination among multiple ministries and departments is vital for the referral of suspected fraud and corruption cases to law enforcement authorities and other relevant bodies. Within existing co-ordination mechanisms, the GPO and AMO have signed co-operation agreements with CCP OLAF, the AA and the CCB that provide a basis for information exchange. There are also co-ordination mechanisms in place to detect and report fraud based on existing risk management practices. The Ministry of Education, Science, Research and Sport, for example, has entered into a co-operation agreement with the PPO and the Government Office of the Slovak Republic: the Ministry actively co-operates with both bodies using lists of risk indicators to detect breaches of competition rules or fraudulent behaviour. In addition, MAs must routinely deal with requests for information from the National Criminal Agency to assist with investigations.

Despite these existing activities and co-ordination mechanisms, MAs and other stakeholders highlighted difficulties in following up with law enforcement authorities regarding the outcomes of reported fraud incidents. Limited communication from these authorities concerning prosecuted cases presents a significant challenge for MAs when reviewing their controls and taking corrective action. Improving the feedback loop regarding prosecution and correction could also enhance fraud risk assessments, reinforce fraud deterrence, and allow MAs to address control vulnerabilities more effectively, reducing the risk of similar fraud incidences occurring in the future. Several Member States have in place measures to foster close co-operation between ESI Funds authorities and investigative and law enforcement bodies (Box 3.5).

Box 3.5. Co-operation with the Financial Crime Investigation Service in Lithuania

In Lithuania, the Financial Crime Investigation Service (FCIS) established a co-operation agreement between the managing authorities, the certifying authority and the audit authority to organise training and workshops. Specifically, FCIS seeks to strengthen the competencies of programme authorities in the management and control of ESI Funds. FCIS shares information about trends in criminal activity and emerging fraud mechanisms and patterns, and suggests preventive measures to reduce recognised control weaknesses. Quarterly meetings are also held with representatives from intermediate bodies, MAs and the Special Investigation Unit, as well as other ministries. These meetings help the participants exchange information on fraud prevention measures, risk assessment processes and anti-fraud tools.

Source: (PWC, 2018[17]), "Compendium of anti-fraud practices for preventing and detecting fraud and corruption in ESI Funds", https://ec.europa.eu/regional_policy/sources/docgener/studies/pdf/implem_article125_compendium_en.pdf.

Key Action: Organise information-sharing forums between authorities responsible for managing ESI Funds and key national authorities, including law enforcement authorities and the Anti-Monopoly Office

There are several opportunities to improve information sharing between law enforcement bodies and entities responsible for fraud and corruption prevention. For instance the former, including the GPO, can regularly attend information-sharing workshops aimed at helping programme authorities identify fraud and corruption trends and patterns and modes of operation. CCP OLAF currently organises at least one training session in co-operation with experienced prosecutors and police investigators from the GPO and National Criminal Agency. The most recent seminar in December 2018 covered criminal activity regarding financial interests in the EU. In addition, law enforcement bodies, as well as other entities such as the GPO and AMO, could participate in the newly formed task force.

The aforementioned entities have access to information that is critical for improving fraud and corruption prevention and detection measures. However, such information is not being used to the fullest possible extent. For example, the GPO circulates information on the outcome of fraud cases with CCP OLAF without any granular data. In addition, representatives from the AMO note that their office monitors ESI Funds and undertakes analyses on beneficial ownership and bid rigging; these analyses could be provided to the MAs and assist them in identifying fraud and corruption risks during the tendering phase of projects. MAs and other programme authorities can benefit from acquiring and analysing information concerning trends in investigation and prosecution, and receiving this information in a timely manner could improve their anti-fraud measures and risk assessments. Specifically, MAs and risk management working groups can use information about schemes and parties involved to inform risk identification as well as risk scoring, so that both are informed by real-world experiences and the results of their own referrals. The sharing of practices is mutually beneficial, as it allows police and law enforcement bodies to build expertise. In turn, this may lead to more effective investigations and prosecutions related to fraud and corruption in EU structural funds.

Priority 5 – Monitor and evaluate fraud risk management activities and controls

Issue analysis

M&E can take place at the government level as well as at the institutional level. In EU-funded project implementation, M&E of fraud risk management is a shared responsibility. It involves the MAs, the AA and working groups. In the Slovak Republic, MAs are at the fifth stage of their risk management programmes, which means they will begin the M&E process in 2019. During this process, risk management working groups for the respective OPs will determine whether the controls implemented are effective by assessing reductions in perceived risks. This M&E process pertains to risk management more broadly but includes a focus on fraud risks and related control activities.

EGESIF and the risk management provisions established for programme authorities provide a basis for M&E of some fraud risk management activities. Given the importance of Key Requirement (KR) 7 during the current programming period, the Slovak Republic has taken steps to ensure that MAs have in place anti-fraud measures that are in line with the components of KR 7. During the M&E process laid out in the respective risk management procedures for OPs, members of the risk management working groups are responsible for assessing whether controls have been effective based on results of risk assessments. This provides insight into how effectively controls are functioning and whether they are commensurate with identified risks; however, this practice constitutes only one part of a comprehensive evaluation of fraud risk management measures and activities within MAs.

As mentioned earlier in this strategy, some of the OP risk catalogues have not captured all relevant fraud and corruption risks. As a result, the monitoring stage of risk management may not accurately capture the reality of which fraud and corruption risks arise within each OP. The current M&E process only assesses identified fraud and corruption risks and implemented controls at the operational level. It does not evaluate the effectiveness of fraud risk assessments, governance structures for managing risks, or other fraud prevention measures. The Slovak Republic is not alone in facing this challenge. From its findings, the European Court of Auditors reports that none of the MAs included in the audit save one examines the effectiveness of their fraud prevention and detection measures, and there are only limited records of which measures are used. As a result, anti-fraud measures are not evaluated in terms of their actual results (European Court of Auditors, 2019[4]).

Although neither the MAs nor the risk management working groups in the Slovak Republic have a systematic or formalised method for undertaking M&E of their risk management practices, some are indeed evaluating the effectiveness of their risk management activities, albeit in an ad hoc manner. Some of the participating MAs have developed methodologies to undertake assessments using techniques such as data harvesting, which are informed by inputs from audit findings and other data sources. However, there appears to be confusion within MAs as to whether or not these methodologies are correct or effective, and in some cases they are not documented. The MAs represented have not developed measurement criteria to monitor and evaluate fraud and corruption risk management activities, which may render evaluations inaccurate and allow deficiencies to go unnoticed in the fifth stage of their risk management programmes.

As of 2019, the EC does not require Member States to systematically assess the horizontal implications of suspected fraud in their MCS, nor does it monitor and evaluate implementation of anti-fraud measures in a comprehensive way. However, in the framework of its revised Anti-Fraud Strategy (European Commission, 2019[28]), the EC is developing profiles of the anti-fraud capabilities of Member States in relation to prevention and detection (European Court of Auditors, 2019[4]). This signals the growing importance of monitoring and evaluating anti-fraud measures, and at this stage provides the Slovak Republic with an opportunity to develop their M&E practices ahead of trends.

Key action: Develop monitoring and evaluation mechanisms, such as scorecards, that capture a wide range of risk management components and activities

To further systematise and integrate M&E activities, the risk management working groups and risk management functions in MAs could benefit from developing targeted, simple tools to structure the evaluation process. These tools can include indicators that help to measure key aspects of anti-fraud policies and risk management practices. This would help ensure that MAs are managing fraud and corruption risks in line with EU policies and regulations, as well as international standards. Moreover, it would support the MAs in their monitoring and evaluation not only of risks, but also of the governance, policies, tools and practices for managing those risks. Easily interpreted templates can help ensure that evaluations capture a range of relevant components of fraud and corruption risk management. Annex A shows a scorecard tailored to the ESI Funds context that can be applied to OPs in the Slovak Republic; however, this tool should be used as a starting point for risk management working groups and MAs to develop their own scorecards in line with their specific needs and risks in their OPs.

Scorecards are typically used to perform organisational self-assessments. They may use a traffic light system or numerical scoring to indicate whether components are functioning properly or require further improvements. For example, in the traffic light system, red indicates that a particular area or factor needs substantial strengthening and improvement, whereas yellow denotes that an area needs a degree of improvement that is not substantive. A green scoring could mean that an area is functioning effectively and does not require improvement (see Table 3.1 and Annex A for examples). These scorecards would ideally cover the key elements of the following areas: fraud and corruption prevention; fraud risk assessment; control activities; corrective action and investigation; and monitoring and evaluation. Assessment of some of these areas may require a more subjective review based on a particular context (e.g. organisational culture) while other areas will be more concrete (e.g. have a documented fraud risk profile). When designing their scorecards, the risk management working groups or functions within MAs can select which scoring system they deem most suitable. Employing numerical scoring may allow for more in-depth assessment, whereas the traffic light system provides an overview of where challenges lie or where fraud risk management activities are functioning effectively.

Table 3.1. Example of a fraud risk management scorecard for monitoring and evaluation

Fraud risk management area/factor	Score	Notes	Action/Responsible actor
Our organisational culture is strong and establishes a zero-tolerance environment with respect to fraud.			
Our authority's top management consistently displays the appropriate attitude regarding fraud prevention and encourages free and open communication regarding ethical behaviour.			
Our authority has an anti-fraud statement to communicate the expected ethical values of staff in the implementation of OPs.			
We have undertaken risk assessment in line with EGESIF and with explicit objectives targeting fraud and corruption risks.			
We have documented the fraud risk profile of the programme following the risk assessment process.			
We have adapted control activities, as necessary, based on the results of the fraud and corruption risk assessment.			
During the risk identification process, our fraud risk assessment individual/team specifically considers the potential for management override of controls, including the controls designed to prevent or detect fraud.			

Source: Developed by OECD; see (COSO, 2016[16]) for additional guidance.

When developing the components of the M&E scorecards, the working groups or risk management functions can use the assessment criteria for Key Requirement (KR) 7 as an initial basis, but it is recommended that the scorecards cover a broader range of measures relating to fraud and corruption risk management (See Annex A). This requires an assessment of the fraud risk management objectives and anti-fraud measures of the MA relating to their OP implementation. Some initial questions to be considered in this exercise include:

- Is fraud risk assessment an integral part of the risk management process?
- Does the assessment of fraud consider fraudulent reporting, possible loss of assets, and corruption resulting from the various ways that fraud and corruption can occur?
- Is regular reporting and monitoring in place in the public organisation relating to its exposure to fraud?
- Are controls and an early warning system in place to identify information signalling new risks that could have a significant impact on the MA?
- Do personnel report through established channels internal control issues to the appropriate internal and external parties in a timely manner, to enable the public organisation to promptly evaluate those issues?
- Does management take adequate and timely actions to analyse and correct deficiencies reported by personnel, internal audit function, or financial and non-financial internal and external monitoring activities?
- Does management monitor the status of corrective actions taken so that they are completed in a timely manner and bring the expected result (e.g. the recommendations of the internal audit or results of monitoring activities)? (Boryczka, Bochnar and Larin, 2019[29])

Key action: Establish measurement criteria to track the performance of fraud risk management activities

Developing measurement criteria enables MAs to benchmark performance against best practices and internal expectations, allowing for continuous improvement of their respective risk management practices. This is reflected in 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 (COSO, 2016[16]). Using defined metrics allows MAs to measure and benchmark actual fraud incidents against the past, providing insights on what is working and what needs further improvement. If there are flaws or gaps in the fraud risk management frameworks of MAs, the speed at which they are discovered can have a critical impact on mitigation. Benchmarking progress and challenges in this way fosters a longer-term view of fraud and corruption prevention in the implementation of OPs. Measurement criteria to track performance of fraud risk management complements the scorecards for M&E, and should be used as inputs for such evaluations.

The primary responsibility for establishing measurement criteria lies with the risk management working groups. For OPs that do not have this structure, the risk management function within the MA could have the primary responsibility. Additionally, the AFCOS-level task force recommended under Priority 1 provides an opportunity for MAs to engage with other programme authorities and utilise their expertise for developing their measurement criteria. For example, CCP OLAF and the CPO can provide targeted inputs for indicators to assess fraud and corruption risk management. When establishing these metrics, a variety of data sources could be considered. Information and data can be drawn primarily but not exclusively from the following sources:

- company registers;
- IMS

- ITMS 2014+
- database maintained by the AMO
- database maintained by the NKU
- database maintained by the PPO
- audit and control reports by the NKU and AA.

Where possible, the measurement criteria should capture the outcome and performance of fraud and corruption risk management, and be in line with the anti-fraud and anti-corruption objectives of MAs. However, considering that risk management is a relatively nascent practice in MAs, data to evaluate the fraud risk management framework may not be readily available and/or measurable, making it more difficult to gauge the outcomes of fraud risk management practices. Where data are unavailable, at a minimum, MAS could assess inputs and outputs for fraud risk management activities. Taking into account the available data sources mentioned above, the risk management working groups or risk management functions within MAs can undertake a mapping exercise to assess what information they can extract from these sources. The initial measurement criteria to be monitored could include:

- the number of irregularities reported as fraudulent in ITMS 2014+ and known fraud or corruption operations committed against programme authorities in the Slovak Republic, including in IBs
- the number of fraud or corruption cases reported to law enforcement authorities by MAs or other public bodies
- the number of allegations of suspected fraud or corruption, both from within MAs and from external actors (i.e. allegations received via whistle-blowing channels)
- the types of fraud and corruption experienced, and resulting losses
- control weaknesses or fraudulent activity uncovered through management verifications and checks or audits
- the number of staff and external parties (i.e. IBs) that have not signed a code of conduct/code of ethics/conflict of interest disclosure
- the number of employees who have not undertaken anti-fraud, anti-corruption or integrity training
- the number of fraud-related audits performed by the relevant audit functions (i.e. internal audit, AA and NKU).

In particular, MAs in the Slovak Republic can make use of reported suspicion of fraud to better assess their internal control systems and fraud risk management frameworks. Box 3.6 provides an example of how Spanish programme authorities have uncovered specific and systematic fraud incidents in OP implementation based on an initial suspicion of fraud.

Box 3.6. Checking for systematic fraud in Spain

Most individual reports of suspected fraud in Spain relating to the 2007-13 programming period can be traced to a single investigation triggered by an intermediate body (IB). Based on the preliminary conclusions of an initial verification, the IB made horizontal checks of all grants awarded to the same final beneficiary. It concluded that there was enough evidence to suspect systematic fraud involving false invoicing and collusion with external suppliers.

The IB duly reported the results of its checks and its suspicion of fraud to the Spanish prosecutors and to the European Commission (EC). The investigation currently covers 73% of all cases of suspected fraud reported in Spain for the 2007- 13 programming period, and 56% of their estimated potential impact on the EU contribution.

Source: European Court of Auditors (2019), *Tackling Fraud in EU Cohesion Spending: Managing Authorities Need to Strengthen Detection, Response and Coordination*, www.eca.europa.eu/Lists/ECADocuments/SR19_06/SR_FRAUD_COHESION_EN.pdf.

Once the measurement criteria have been established, the risk management working groups or functions can undertake comparative analyses to aid their M&E of fraud risk management, and identify challenges or successes. For example, the measurement criteria can be used to compare types of fraudulent irregularities and cases of fraud and corruption with those previously detected during project implementation. It can also be used to inform the scorecard evaluation, the results of which could be communicated to senior management to ensure that resources are allocated in proportion to risk management activities and to remediate deficiencies.

Proposals for action

Towards adopting a systematic approach to fraud risk management

Action	Description	Entity/entities with the primary responsibility	Time frame (short, medium, long term)
1	Have managing authorities develop and approve a tailored anti-fraud policy and disseminate it widely	MAs	Short
2	Create a task force in the AFCOS network to enable knowledge sharing and exchange of good practices between managing authorities and key stakeholders	CCP OLAF and risk management working groups	Short
3	Develop formalised, regular, and ongoing training programmes on fraud risk management and assessments for personnel in managing authorities	MAs and CCP OLAF	Medium/long
4	Organise information-sharing forums between authorities responsible for managing ESI Funds and key national authorities, including law enforcement authorities and the Anti-Monopoly Office	CCP OLAF	Short/medium
5	Develop monitoring and evaluation mechanisms, such as scorecards, that capture a wide range of risk management components and activities	Risk management working groups, MAs	Medium
6	Establish measurement criteria to track the performance of fraud risk management activities	Risk management working groups, MAs	Medium

Annex A. **A comprehensive fraud risk management scorecard for managing authorities**

Fraud risk governance area/factor	Score	Notes	Action/Responsible actor
Our organisational culture is strong and establishes a zero-tolerance approach to fraud and corruption.			
Our senior management consistently displays the appropriate attitude regarding fraud prevention and encourages free and open communication regarding ethical behaviour.			
Our entity has an anti-fraud policy that communicates the expected ethical values of staff in the implementation of OPs.			
Our anti-fraud policy is tailored to our specific risk profile and considers relevant fraud risk scenarios involving ESI Funds.			
Staff within our entity are provided with regular training in fraud and corruption risks.			
Our entity has reporting channels in place that are communicated to staff.			

Fraud risk assessment area/Factor	Score	Notes	Action/Responsible actor
We have undertaken risk assessment in line with EGESIF and with explicit objectives targeted at fraud and corruption risks.			
Our fraud risk assessment team includes all appropriate levels of management and internal and external sources.			
We use a fraud risk assessment matrix to identify and document the specific areas of greatest risk to our entity and to help us determine how to tailor the assessment process accordingly.			
Our fraud risk assessment team gathers information about potential fraud from internal sources, such as interviews with personnel, complaints received from the whistleblower hotline, and analytical procedures.			
We accord high priority to those fraud risks we deem to be highly likely and highly significant in relation to our OP.			
Our management assesses the likelihood of a fraud risk materialising by determining instances in which the particular fraud has occurred in our entity in the past, the prevalence of the particular fraud risk in the ESI Funds context, and other factors.			
During the risk identification process, our fraud risk assessment individual/team specifically considers the potential for management override of controls, including the controls designed to prevent or detect fraud.			
Our fraud risk assessment team consults with relevant actors from other entities to inform risk assessments, i.e. CPO, PPO.			

We use any of the following data analytics techniques to gather fraud risk evidence: • data stratification • risk scoring • trend analysis • data visualisation • statistical and predictive modelling • information from external sources in analytics.			
We have adapted control activities as necessary, based on the results of the fraud and corruption risk assessment.			
We have documented the fraud risk profile of the programme following the risk assessment process.			

Fraud control activities area/Factor	Score	Notes	Action/Responsible actor
If the fraud risk assessment revealed that existing control activities are not sufficient to reduce fraud risk to an acceptable level, management has effectively addressed this issue by selecting, developing and implementing additional controls to supplement or replace the existing ones.			
We select our fraud control activities in response to entity-specific factors and relevant business processes.			
Our control activities adequately mitigate the risk of fraud in accordance with our entity's specific risk tolerance.			
Our entity assesses and continuously monitors detective controls to verify that our fraud and corruption detection techniques are present and functioning, and to ensure that fraud that is occurring or has occurred is detected in a timely manner.			
We formally document our fraud risk management policies and procedures, such as the control activities in place to prevent and detect fraud.			
Our fraud documentation includes the processes used to monitor the performance of fraud control activities, and indicates when these controls do not sufficiently reduce risk to an acceptable level.			

Fraud response/Investigation area/Factor	Score	Notes	Action/Responsible actor
Our entity stresses the importance of having a documented process in place through which allegations of fraud are to be consistently captured, assessed, and responded to in a timely manner.			
Our fraud investigation and response system includes protocols for: • updating a central repository for allegations and complaints • maintaining the anonymity or confidentiality of the individuals involved, except as necessary to investigate • initially evaluating the allegations to determine if an investigation is warranted and the appropriate degrees of urgency • notifying employees regarding document preservation and securing data systems • if necessary, engaging independent counsel and forensic accounting support • conducting the investigation while controlling and safeguarding evidence			

• reporting the results in the appropriate format (oral summary of key points or comprehensive written report with exhibits) • following policies regarding retention of reports, documents, work papers and other information • Assessing root causes and initiating mitigating processes and controls.			
We advise the Audit Authority at the appropriate time of any alleged fraud that could affect our financial statements.			
We report suspicions of fraud to law enforcement agencies in a timely manner.			
We communicate regularly with law enforcement agencies once fraud cases have been referred to them.			

Fraud risk management monitoring and evaluation (M&E) area/Factor	Score	Notes	Action/Responsible actor
We document our plan, approach, and scope for monitoring our entity's fraud risk management practices.			
The Risk Management Working Group for our OP has developed tools to facilitate M&E of fraud risk management, e.g. scorecards.			
We have established measurement criteria to monitor and improve fraud prevention and detection.			
We provide the established measurement criteria to monitor and improve fraud prevention and detection to our entity's leadership on an ongoing basis.			
Our ongoing monitoring activities include data analytics techniques.			
We closely monitor emerging fraud and corruption schemes involving ESI Funds and determine whether our entity is protected against such cases. We remediate, in a timely manner, any deficiencies identified in our fraud risk management framework as a result of M&E activities.			

Annex B. The chronology of proposed actions for the Government of the Slovak Republic

Table A B.1. Key actions for enhancing fraud and corruption risk assessments

Action	Description	Entity/entities with the primary responsibility	Time frame (short, medium, long term)
1	Review and update risk assessment procedures to ensure greater clarity for identifying fraud and corruption risks across the ESI Funds project cycle	MAs/risk management working groups or risk management functions within MAs	Short
2	Clarify and improve the criteria for scoring fraud and corruption risks	MAs/risk management working groups or risk management functions within MAs	Short
3	Ensure control activities are appropriate, sufficient and proportional to identified risks	MAs/risk management working groups or risk management functions within MAs	Short
4	Further define objectives and expand the use of Arachne for assessing risks within MAs, with practical guidance from the CCB	MAs/CCB	Medium
5	Conduct periodic statistical analysis of irregularities, fraud cases and audit findings to help determine higher-risk areas in different sectors across the whole system	CCP OLAF/MAs	Medium
6	Develop a plan for more effective use of data on irregularities and public procurement	MAs/CCB	Long

Table A B.2. Key actions for adopting a systematic approach for managing fraud and corruption risks

Action	Description	Entity/entities with the primary responsibility	Time frame (short, medium, long term)
1	Have managing authorities develop and approve a tailored anti-fraud policy and disseminate it widely	MAs	Short
2	Create a task force in the AFCOS network to enable knowledge sharing and exchange of good practices between managing authorities and key stakeholders	CCP OLAF and risk management working groups	Short
3	Organise information-sharing forums between authorities responsible for managing ESI Funds and key national authorities, including law enforcement authorities and the Anti-Monopoly Office	CCP OLAF	Short/medium
4	Develop monitoring and evaluation mechanisms, such as scorecards, that capture a wide range of risk management components and activities	Risk management working groups, MAs	Medium
5	Establish measurement criteria to track the performance of fraud risk management activities	Risk management working groups, MAs	Medium
6	Develop formalised, regular, and ongoing training programmes on fraud risk management and assessments for personnel in managing authorities	MAs and CCP OLAF	Medium/long

References

Boryczka, M., D. Bochnar and A. Larin (2019), "Guidelines for assessing the quality of internal control systems", *SIGMA Papers*, No. 59, OECD Publishing, Paris, https://dx.doi.org/10.1787/2a38a1d9-en. [29]

COSO (2016), *Fraud Risk Management Guide*, The Committee of Sponsoring Organizations of the Treadway Commission, https://www.coso.org/Pages/Purchase-Guide.aspx. [16]

Department for Communities and Local Government (2015), *Lifecycle of a Project: 2014-2020 European Structural and Investment Funds Growth Programme*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/592187/ERDF_and_ESF_Lifecycle_of_a_Project_270715_v2.pdf. [7]

European Commission (2019), *Commission Anti-Fraud Strategy: Enhanced Action to Protect the EU Budget*, https://ec.europa.eu/anti-fraud/sites/antifraud/files/2019_commission_anti_fraud_strategy_en.pdf. [28]

European Commission (2018), *29th Annual Report on the Protection of the European Union's Financial Interests: Fight against Fraud, 2017*, https://ec.europa.eu/anti-fraud/sites/antifraud/files/pif_report_2017_en.pdf. [3]

European Commission (2017), *Arachne Frequently Asked Questions*, https://ec.europa.eu/social/BlobServlet?docId=15097&langId=en. [21]

European Commission (2017), *Follow-up of Recommendations to the Commission Report on the Protection of the EU's Financial Interests: Fight against Fraud, 2015*, https://ec.europa.eu/anti-fraud/sites/antifraud/files/2_autre_document_travail_service_part1_v2_en.pdf. [25]

European Commission (2017), *Special Eurobarometer 470 - Corruption*, http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/81007. [5]

European Commission (2015), *European Structural Investment Funds: Guidance for Member States on Management Verifications (2014-2020)*, https://ec.europa.eu/regional_policy/sources/docgener/informat/2014/guidance_management_verifications_en.pdf. [22]

European Commission (2015), *Investing in Jobs and Growth: Maximising the Contribution of European Structural and Investment Funds*, https://ec.europa.eu/regional_policy/en/information/publications/communications/2015/investing-in-jobs-and-growth-maximising-the-contribution-of-the-european-structural-and-investment-funds. [1]

European Commission (2014), *Assessment of Exposure to Specific Fraud Risks by Managing Authorities*, https://ec.europa.eu/regional_policy/en/information/publications/guidelines/2014/fraud-risk-assessment-and-effective-and-proportionate-anti-fraud-measures. [15]

European Commission (2014), *European Structural and Investment Funds Country Factsheet - Slovakia*, https://ec.europa.eu/regional_policy/en/information/publications/factsheets/2016/european-structural-and-investment-funds-country-factsheet-slovakia. [8]

European Commission (2014), *Guidance for Member States and Programme Authorities on Fraud Risk Assessment and Effective and Proportionate Anti-Fraud Measures*, https://ec.europa.eu/regional_policy/sources/docgener/informat/2014/guidance_fraud_risk_assessment.pdf. [14]

European Commission (2014), *Guidance for the Commission and Member States on a Common Methodology for the Assessment of Management and Control Systems in the Member States*, https://ec.europa.eu/regional_policy/en/information/publications/guidelines/2014/guidance-for-the-commission-and-member-states-on-a-common-methodology-for-the-assessment-of-management-and-control-systems-in-the-member-states. [26]

European Commission (n.d.), *Europe 2020 Strategy*, https://ec.europa.eu/info/business-economy-euro/economic-and-fiscal-policy-coordination/eu-economic-governance-monitoring-prevention-correction/european-semester/framework/europe-2020-strategy_en (accessed on 3 May 2019). [6]

European Court of Auditors (2019), *Tackling fraud in EU Cohesion Spending: Managing Authorities Need to Strengthen Detection, Response and Coordination*, http://publications.europa.eu/webpub/eca/special-reports/fraud-in-cohesion-6-2019/en/#chapter3. [4]

European Parliament (2017), *Directive (EU) 2017/1371 on the fight against fraud to the Union's financial interests by means of criminal law*. [12]

European Parliament (2013), *Regulation (EU) No 1303/2013 of the European Parliament and of the Council of 17 December 2013 laying down common provisions on the European Regional Development Fund, the European Social Fund, the Cohesion Fund, the European Agricultural Fund for Rural D*. [27]

European Union (2016), *Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union (TFEU) [2016] OJ C202/1*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT (accessed on 3 May 2019). [13]

GAO (2015), *A Framework for Managing Fraud Risks in Federal Programs*, https://www.gao.gov/assets/680/671664.pdf (accessed on 3 May 2019). [19]

Government of the Slovak Republic (2014), *National Strategy for the Protection of the European Union's Financial Interests in the Slovak Republic*. [11]

Höslová, M. (2015), *Irregularities in EU projects and their Solution*, https://dspace5.zcu.cz/handle/11025/18262. [10]

ISO (2018), *ISO 31000 - Risk Management Guidelines*, https://www.iso.org/iso-31000-risk-management.html. [24]

KPMG (2016), *EU Funds in Central and Eastern Europe: Progress Report 2007-2015*. [9]

OECD (2019), *Analytics for Integrity: Data-Driven Approaches for Enhancing Corruption and Fraud Risk Assessments*, OECD, http://www.oecd.org/gov/ethics/analytics-for-integrity.pdf. [18]

OECD (2017), *Internal Control and Risk Management for Public Integrity in the Middle East and North Africa*, OECD, https://www.oecd.org/gov/ethics/corruption-risks-internal-control-mena.pdf. [20]

PWC (2018), *DG REGIO – Preventing Fraud and Corruption in the European Structural and Investment Funds: Taking Stock of Practices in the EU Member States*, https://ec.europa.eu/regional_policy/sources/docgener/studies/pdf/implem_article125_en.pdf. [17]

Teffer, P. (2018), *Fraudsters Lured by EU Structural Funds*, EUobserver, https://euobserver.com/regions/142195. [2]

The Chartered Institute of Public Finance & Accountancy (2014), *Code of Practice on Managing the Risk of Fraud and Corruption*, CIPFA \ The Chartered Institute of Public Finance and Accountancy, https://www.cipfa.org/~/media/files/cipfa%20thinks/reports/cipfa%20code%20of%20practice%20on%20managing%20the%20risk%20of%20fraud%20and%20corruption.pdf. [23]

Further reading

Government of Australia (n.d.), Fraud and Corruption Control Plan 2016-2018, Department of the Prime Minister and Cabinet, https://www.pmc.gov.au/sites/default/files/files/pmc/Fraud-Control-Plan.docx (accessed on 03 May 2019).

European Commission and PricewaterhouseCoopers (2018), DG REGIO-Preventing fraud and corruption in European Structural and Investment Funds-taking stock of practices in the EU Member States: Compendium of anti-fraud practices for preventing and detecting fraud and corruption in ESI Funds, https://ec.europa.eu/regional_policy/sources/docgener/studies/pdf/implem_article125_compendium_en.pdf.

European Court of Auditors (2019), *Special Report - Fighting fraud in EU spending: Action needed*, https://www.eca.europa.eu/Lists/ECADocuments/SR19_01/SR_FRAUD_RISKS_EN.pdf.

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

The Institute of Risk Management (2012), *Risk culture - Resources for Practitioners*, https://www.theirm.org/media/3814165/Risk-Culture-Resources-for-Practitioners.pdf (accessed on 02 April 2019).

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

The OECD is a unique forum where governments work together to address the economic, social and environmental challenges of globalisation. The OECD is also at the forefront of efforts to understand and to help governments respond to new developments and concerns, such as corporate governance, the information economy and the challenges of an ageing population. The Organisation provides a setting where governments can compare policy experiences, seek answers to common problems, identify good practice and work to co-ordinate domestic and international policies.

The OECD member countries are: Australia, Austria, Belgium, Canada, Chile, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea, Latvia, Lithuania, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The European Union takes part in the work of the OECD.

OECD Publishing disseminates widely the results of the Organisation's statistics gathering and research on economic, social and environmental issues, as well as the conventions, guidelines and standards agreed by its members.

OECD PUBLISHING, 2, rue André-Pascal, 75775 PARIS CEDEX 16
ISBN 978-92-64-56816-7 – 2019

OECD Public Governance Reviews

Tackling Fraud and Corruption Risks in the Slovak Republic

A STRATEGY WITH KEY ACTIONS FOR THE EUROPEAN STRUCTURAL AND INVESTMENT FUNDS

This report outlines a strategy for managing fraud and corruption risks related to the European Structural and Investment (ESI) Funds in the Slovak Republic. It suggests targeted and tailored actions for the authorities responsible for these funds, building on their existing fraud and corruption risk management practices. The strategy and key actions draw from the *OECD Recommendation of the Council on Public Integrity*, as well as European Commission guidance and international standards of *inter alia* the Committee of Sponsoring Organizations of the Treadway Commission (COSO), Institute of Internal Auditors (IIA) and International Organization for Standardization (ISO).

Consult this publication on line at ***https://doi.org/10.1787/6b8da11a-en***.

This work is published on the OECD iLibrary, which gathers all OECD books, periodicals and statistical databases. Visit ***www.oecd-ilibrary.org*** for more information.

OECD publishing
www.oecd.org/publishing

ISBN 978-92-64-56816-7