IQ-Net

Improving the quality of Structural Funds management

IS FRAUD RISK MANAGEMENT IN COHESION POLICY EFFECTIVE AND PROPORTIONATE?

Viktoriya Dozhdeva and Carlos Mendez

Report for the 49th IQ-Net Conference (Online), 3 December 2020

Registered address:
Stichting EPRC Delft
Faculty of Architecture and the Built Environment,
Technische Universiteit Delft
Julianalaan 134
2628 Delft
Netherlands

T: +44-141-548-3908
E: info@eprcdelft.eu
W: https://eprc-strath.org/eu/

Stichting EPRC Delft is a non-profit foundation registered in the Netherlands (No. 69203288)

PREFACE

The IQ-Net Network promotes exchange of experience on the management and implementation of Structural Funds programmes among managing authorities and intermediate bodies. The network is managed by the European Policies Research Centre Delft under the direction of Professor John Bachtler and Heidi Vironen. The research for this report was undertaken by EPRC in preparation for the 49th IQ-Net Conference (online) on 3 December 2020. The report was written by Viktoriya Dozhdeva and Dr Carlos Mendez.

The report is the product of desk research and fieldwork during Autumn 2020 with national and regional authorities in EU Member States (notably partners in the IQ-Net Consortium). The field research team comprised:

- Stefan Kah (Austria)
- Dr Wilbert den Hoed (Belgium, the Netherlands)
- Dr Vinko Muštra (Croatia)
- Dr Marie Feřtrová (Czechia)
- Lise Smed Olsen (Denmark)
- Heidi Vironen (Finland)
- Liliana Fonseca (France)
- Fabian Gal (Germany)
- Dr Eleftherios Antonopoulos (Greece)
- Dr Martin Ferry (Poland)
- Viktoriya Dozhdeva (Portugal)
- Neli Georgieva (Slovakia)
- Dr Carlos Mendez (Spain)
- Rona Michie (United Kingdom)

EPRC thanks all those respondents from national and regional authorities and the European Commission who participated in the research. Thanks also to Jayne Ogilvie, who contributed to the data visualisations in this paper. Additionally, EPRC gratefully acknowledges the financial support provided by participating national and regional authorities, whose contributions are partly co-financed by Technical Assistance from the European Structural and Investment Funds.

The partners in the IQ-Net network are as follows:

Austria

- ÖROK Secretariat – Austrian Conference on Spatial Planning

Belgium

- Enterprise Agency Flanders

Croatia

- Ministry of Regional Development & EU Funds

Czechia

- Ministry of Regional Development

Denmark

- Danish Business Authority

Finland

- South and West Finland (Etelä- ja Länsi-Suomi)

Germany

- Nordrhein-Westfalen (North Rhine-Westphalia), Ministry for Economic Affairs, Innovation, Digitalization and Energy

Greece

- Management Organisation Unit of Development Programmes S.A.

Netherlands

- Managing Authority Kansen voor West
- Managing Authority Noord, Northern Netherlands Alliance (SNN)
- Managing Authority OP Oost
- Managing Authority Stimulus (OP Zuid)

Poland

- Marshal Office of the Pomorskie Region
- Marshal Office of the Warmińsko-Mazurskie Region

Portugal

- Agency for Development and Cohesion (ADC)

Spain

- Provincial Council of Bizkaia / País Vasco (Basque Country)

Slovakia

- Ministry of Investments, Regional Development and Informatization of the Slovak Republic

United Kingdom

- Ministry of Housing, Communities and Local Government (England)
- Scottish Government
- Welsh European Funding Office

For further information about IQ-Net, and access to the full series of IQ-Net Papers, please visit the IQ-Net website at: http://www.eprc-strath.eu/iqnet.

To cite this paper, please use the following: Dozhdeva V and Mendez C (2020) *Is Fraud Risk Management in Cohesion Policy Effective and Proportionate?* IQ-Net Thematic Paper 47(2), European Policies Research Centre Delft.

Disclaimer

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

AA	Audit Authority
AFCOS	Anti-Fraud Coordination Service
CA	Certifying Authority
CF	Cohesion Fund
COCOLAF	Advisory Committee of the Member States for the Coordination of Fraud Prevention
CPR	Common Provisions Regulation
DG	Directorate General
EC	European Commission
ERDF	European Regional Development Fund
ESF	European Social Fund
ESIF	European Structural and Investment Funds
FRA	Fraud Risk Assessment
FRM	Fraud Risk Management
IB	Intermediate Body
IROP	Integrated Regional Operational Programme (Czech Republic)
MA	Managing Authority
(P)MC	(Programme) Monitoring Committee
MCS	Management and Control System
MFF	Multi-annual Financial Framework
MS	Member State
OLAF	European Anti-Fraud Office
OP	Operational Programme
PA	Partnership Agreement
ROP	Regional Operational Programme
SCO	Simplified Cost Options
TA	Technical Assistance
TO	Thematic Objective

COUNTRY/PROGRAMME ABBREVIATIONS

Country	Abbreviation
Austria	AT
Belgium (Vlaanderen)	BE (Vla)
Croatia	HR
Czechia	CZ
Denmark	DK
Finland	FI
France	FR
Germany	DE
Germany (Nordrhein-Westfalen)	DE (NRW)
Greece	EL
Netherlands	NL
Poland	PL
Poland (Pomorskie)	PL (Pom)
Poland (Warmińsko-Mazurskie)	PL (W-M)
Portugal	PT
Slovakia	SK
Spain	ES
Spain (Bizkaia, País Vasco)	ES (Biz)
United Kingdom	UK
United Kingdom (England)	UK (Eng)
United Kingdom (Scotland)	UK (Sco)
United Kingdom (Wales)	UK (Wal)

EXECUTIVE SUMMARY

Fraud risk management of European Structural and Investment Funds has acquired increased salience in recent years in the context of criticism about the effectiveness and misuse of EU funding, a more robust regulatory framework and anti-fraud strategy by the European Commission and proactive efforts by some Member States to tackle fraud and corruption.

While reported levels of fraud are relatively low, fraud and corruption can still undermine the effectiveness and efficiency of the Funds, create reputational damage to the EU and the Member States, and undermine citizens' trust in Cohesion Policy. Effective anti-fraud strategies can, in principle, strengthen the quality of Cohesion policy governance and contribute to economic, social and territorial development.

The 2014-20 regulatory framework has introduced a more structured prevention and detection approach against fraud and corruption in Cohesion Policy with obligations to put in place effective and proportionate anti-fraud measures. The evolution of the regulatory approach means that fraud risk management is now seen as a strategic function with a stronger role for fraud risk assessment to underpin anti-fraud measures, a clear specification of institutional responsibilities and coordination, along with targeted resources and tools. It has promoted more active discussion, development of new skills, greater transparency and a more integrated approach. New opportunities have also been provided by electronic tools for identifying fraud risk.

While the evolution of fraud risk management is assessed positively overall, challenges remain and assessments of specific measures are mixed across different countries and regions. There is still scope for improving coordination in many cases through the establishment of central coordination bodies/responsibilities, platforms for information exchange and advice sharing, better cooperation with law-enforcement and prosecution bodies, as well as harmonisation of methodological guidance on fraud risk management. Some authorities face capacity and human resource constraints particularly given the expansion of fraud management responsibilities and requirements, competing tasks, deadlines and time constraints, and insufficient awareness of what constitutes fraudulent irregularities.

The main lessons drawn from the current period for the 2021-27 period are fivefold:

- **the need for greater cooperation, harmonisation and interoperability**, among the different information systems, institutions and actors;

- **simplification**, particularly to decrease administrative burden;
- **flexibility and proportionality**, in the sense of providing scope to adapt the rules and systems to the specific domestic operating and legal contexts;
- **the need to enhance the anti-fraud capacity-building**, including in terms of resource allocation, training, information and guidance; and
- **the need for a greater focus on early detection and prevention**, including via enhanced risk assessment mechanisms.

For the 2021-27 period, continuity in fraud risk management approaches is expected in many cases, along with ongoing improvements to IT tools and institutional coordination. While some IQ-Net programme managers do not expect significant implications from the regulatory flexibility introduced to deal with the consequences of Covid-19 and additional funding through REACT-EU for fraud prevention, risk analysis, control and detection, others have already seen an increase in fraudulent activities or anticipate additional pressures in the near future. In order to mitigate and address these challenges, new awareness-raising, training and capacity-building actions are foreseen along with revisions of sanctions and simplification of control procedures.

More generally, there are wider necessary preconditions for robust and proactive fraud risk management in the current and future periods, not least in terms of promoting awareness, cultures and mind-sets among managing authorities, implementation bodies and beneficiaries in the face of multiple and often conflicting administrative pressures and priorities to spend funding effectively and efficiently. The scale of fraud risks also varies across countries and regions depending on the relative scale of funding, types of expenditure supported, the quality of institutions and political commitment to tackling fraud.

1 INTRODUCTION

"The first thing I did when I began my job is to ask for the numbers in terms of the fraudulent use of funds from the last completed Multiannual Financial Framework, which ended in 2014 – the figure was less than 1%...But this is not the image people have – the public have an image of massive fraud"

Commissioner Ferreira, Interview in the New Federalist, 16 October 2020

Fraud risk management has acquired increased salience in the management of EU Cohesion Policy and EU budgetary expenditure in general. While reported levels of fraud are relatively low, fraud and corruption can still undermine the effectiveness and efficiency of the Funds, create reputational damage to the EU and the Member States, and undermine citizens' trust in Cohesion Policy. Effective anti-fraud strategies can, in principle, strengthen the quality of Cohesion policy governance and contribute to economic, social and territorial development.

The 2014-20 regulatory framework has introduced a more structured prevention and detection approach against fraud and corruption in shared management with obligations to put in place effective and proportionate anti-fraud measures. The evolution of the regulatory approach means that fraud risk management is now seen as a strategic function. It requires stronger ex-ante and ongoing assessment to underpin effective and proportionate anti-fraud measures, a clear specification of institutional responsibilities and coordination, along with resources and tools.

Nevertheless, the implementation of effective and proportionate risk management systems and measures is uneven and faces important challenges, not least in terms of the associated administrative burden, coordination challenges, capacity deficits, and, in some cases, the absence of a strong anti-fraud culture.

Against this background, the following paper takes stock of how fraud risk management of Structural Funds is evolving across different contexts. Drawing on research from IQ-Net countries and regions, it reviews fraud risk management implementation experiences, identifies examples of good practice, and explores the factors contributing to effective and proportionate fraud risk management strategies and measures. Lastly, it identifies questions as a basis for discussion at the IQ-Net conference.

2 THE POLICY AND REGULATORY CONTEXT

2.1 The scale of fraud

Reported fraud in Cohesion Policy is relatively low as a share of funding allocations and in terms of the number of cases, although it is difficult to estimate levels of undetected fraud. The latest annual report on the protection of the EU's financial interests and the fight against fraud for the 2019 financial year shows that irregularities reported as fraudulent by Member States (the so-called 'fraud detection rate') in 2007-13 represent 0.44 percent of Cohesion Policy expenditure, with significant variations across Member State – ranging from 0 percent (Ireland, Luxembourg, Sweden) to 1.17 percent (Slovakia).[1] For 2014-20, the high fraud detection rate reported for Slovakia is accounted for by just two irregularities valued at 0.64 billion (mainly ERDF) which account for most of the total value of reported fraud across all countries and skew the overall results. The two cases were at an early stage in the fraud management process at the time of reporting and may change.

Data on fraud needs to be treated with caution. The main source is the obligatory reporting from Member States on detected, suspected and established fraud in the Irregularity Management System (IMS) managed by OLAF. The European Commission treats these figures with caution for the following reasons:

- the figures are highly dependent on the accuracy and completeness of reporting made by Member State, and are likely to be under-reported;
- other sources suggest that the scope of fraud and/or corruption particularly in public procurement (part of which is EU co-financed) may be greater than the reporting by Member States;
- a large share of Cohesion Policy spending is on discretionary and high value public contracts (e.g. infrastructure), which studies suggest can have higher risks of corruption;
- average figure masks striking differences between Member States and regions; and
- temporal trends many not be reliable indicators of performance due to changes in regulatory requirements and increased awareness of obligations.

Table 1: Fraud Detection Rate (FDR) in 2007-13 and 2014-20

Country	FDR 2007-13	FDR 2014-20
AT	0.14%	0.06%
BE	0.02%	0.00%
BG	0.10%	0.02%
HR	0.28%	0.05%
CY	0.18%	0.00%
CZ	0.92%	0.04%
DK	0.04%	0.39%
EE	0.31%	0.06%
FI	0.02%	0.07%
FR	0.02%	0.19%
DE	0.12%	0.04%
GR	0.47%	0.20%
HU	0.04%	0.19%
IE	0.00%	0.00%
IT	0.39%	0.00%
LV	0.80%	0.57%
LT	0.03%	0.02%
LU	0.00%	0.00%
MT	0.04%	0.00%
NL	0.26%	0.04%
PL	0.63%	0.14%
PT	0.71%	0.02%
RO	1.07%	0.13%
SK	1.17%	23.36%
SI	0.68%	0.02%
ES	0.06%	0.00%
SE	0.00%	0.04%
UK	0.13%	0.04%
EU28	0.44%	0.79%

Source: European Commission (2020) PIF 2019

The most common types of fraudulent irregularities are classified as infringements of contract provisions/rules; infringements of public procurement rules; incorrect, missing, false or falsified supporting documents; and ethics and integrity. There is a particularly high prevalence of fraudulent irregularities in the priority 'RTDI, innovation and entrepreneurship' in 2014-20, which accounts for over 90 percent of the value of fraud, followed by the priorities 'Environment protection and risk prevention' and 'Improving access to employment and sustainability'. A recent OECD report on Fraud and Corruption in ESIF identifies the main risk across three phases of the project cycle (Table 2).

Table 2: Common fraud and corruption risks during the project cycle

Project cycle	Fraud and corruption risks
Project application and selection	- Conflict of interest - Influence peddling - Bribery - Unfairly awarding projects - Manipulating documents
Project implementation	- Avoiding genuine competition - Manipulating documents - Creating fictitious companies - Withholding documents - Inflating staff costs - Modifying Contract Data - Fabricating fictitious works - Providing faulty products - Substituting products - Bid-rigging - Bribery - Collusive bidding
Project closure and evaluation	- Conflict of interest - Forging documents - Bribery

Source: Adapted from OECD (2019) Fraud and corruption in European Structural and Investment Funds: A spotlight on common schemes and preventive actions. OECD, Paris.

2.2 Fraud risk management responsibilities

The Commission and the Member States share responsibility to counter fraud and other illegal activities affecting the EU's financial interests. However, Member States have the main responsibility for tackling fraud as national authorities are responsible for managing and implementing ESIF programmes. Member States are responsible for the prevention, detection and correction of irregularities, including fraud, and for the recovery of funds unduly paid. This requirement is more explicit in the Common Provisions Regulation (CPR) for the 2014-20 period compared to 2007-13, requiring MAs to "put in place effective and proportionate anti-fraud measures taking into account the risks identified". The Commission recommends that MAs adopt a structured approach across the full anti-fraud management cycle comprising fraud prevention, detection, correction and prosecution.

Member State responsibilities

- **Management and control systems.** Member States' management and control systems are required to protect the EU's financial interests and in particular to prevent, detect and correct irregularities, including fraud, and to recover funds unduly paid to beneficiaries (Art 72, CPR). In particular, fraudulent irregularities are mainly detected by first-level management checks, including on-the-spot checks by MAs and audits of projects by audit authorities.

- **Reporting to the Commission.** Member States are required to report to the Commission detected irregularities and the associated preventive and corrective measures in cases of suspected fraud (Art.122, CPR).

- **MA anti-fraud strategy.** A key requirement listed under MA functions is to put in place effective and proportionate anti-fraud measures taking into account the risks identified (Art. 125, CPR).

- **Capacity building.** Member States can also invest EU funds in administrative capacity to tackle fraud through TO11 - Strengthening institutional capacity and efficient public administration; or through the Technical Assistance priority axis of OPs e.g. by funding staff costs on audit activity or through investments in anti-fraud systems and tools.

European Commission responsibilities

The European Commission's DGs are required to ensure that the Member States have set up, and effectively run management and control systems to make sure funds are used efficiently and correctly to ensure legality and regularity of expenditure.

- **Supervision of management and control.** The DGs carry out audits in the Member States to verify the effective functioning of national systems in the framework of a multi-annual audit strategy. ESIF DGs single audit strategy contributes to anti-fraud efforts through the verification of the effectiveness of the management and control systems in Member States.

- **Cooperation with OLAF.** Whenever the DGs' auditors encounter a potential case of fraud, the information is transmitted to the European Anti-Fraud Office (OLAF) for assessment and investigation. Further cooperation/exchange of information with OLAF includes:

    - annual meetings of the Directors-General;
    - follow-up of OLAF cases;
    - contributions to the Commission's Fraud Prevention and Detection Network (FDP-Net) as well as to COCOLAF (Advisory Committee of the member States for the Coordination of Fraud Prevention, chaired by OLAF);
    - fraud-proofing of legislation;
    - publication of OLAFs Annual PIF Report, including a statistical evaluation of irregularities/fraud;
    - OLAF assistance in training events;
    - informing about investigations; and
    - guidance by OLAF to DGs and Member States and methodologies.

3 FRAUD RISK MANAGEMENT APPROACHES IN 2014-20

3.1 Key strategic and operational developments

ESIF fraud risk management regulatory provisions have become wider in scope and more formally regulated with a greater role for anti-fraud measures within the wider framework of management and control systems. The evolution of the regulatory approach means that fraud risk management is now seen as a strategic function, requiring stronger ex-ante and ongoing assessment to underpin effective and proportionate anti-fraud measures, a clear specification of institutional responsibilities and coordination, along with resources and tools. The question for this section is how these expectations are being translated into practice on the ground.

In line with Commission guidance, a number of IQ-Net authorities have **established specific anti-fraud policy statements and strategies** or cover Cohesion Policy in **wider national anti-fraud strategies** to protect the EU's financial interests more generally.

Croatia. The National Anti-Fraud Strategy for the Protection of the EU's Financial Interests for the period 2014-2016 was adopted by the Government of the Republic of Croatia on 23 January 2014 and represents the main strategic document outlining priorities and measures taken to protect the EU's financial interests Croatia. The Croatian Parliament adopted the Anti-Corruption Strategy for the period 2015-2020 on 27 February 2015. On the basis of that Strategy, the Action Plan for 2015 and 2016 and the Action Plan for 2017 and 2018 were adopted.

France: A national anti-fraud strategy is established practice. In April 2008, the National Anti-Fraud Unit (DNLF) was created by order of the French Prime Minister and the French Minister for Finance, Public Funds and State Reform. In 2020, the DNLF was dismantled and replaced by the Inter-ministerial Anti-Fraud Coordination Mission (MICAF). The DNLF acted as a secretary to the National Anti-Fraud Committee (CNLF), being responsible for organising the fight against tax and social fraud and illegal labour. It was in charge of the national coordination plan for the fight against fraud in public finances. The plan was devised in 2016, and it constituted an inter-ministerial anti-fraud roadmap relating to all public, national and European funding, providing an integrated and comprehensive approach to combatting fraud.

Greece: The General Secretariat for Public Investments – Partnership Agreement has declared a zero-tolerance policy on fraud. This policy has been crystalized into a "National Anti-Fraud Strategy for Structural Actions", issued in 2014 and revised in 2017. Addressing EU regulatory requirements, the strategy and the Action Plan for its implementation was developed by the General Secretariat for Public Investments and PA, via the Special Service for Institutional Support in cooperation with the Audit Authority, the Economic Crime Unit (SDOE) and the Greek Anti-Fraud Coordination Service (AFCOS).

The Netherlands: Responding to the European Commission's recommendation to develop a national anti-fraud strategy, the Dutch Ministry of Finance organised a strategic meeting to outline the organisational structure and responsibilities for combating fraud. The meeting has brought the various anti-fraud actors together,

including prosecution bodies such as the Fiscal Information and Investigation Service (*FIOD*), the police, tax authorities and the national and ESIF aid granting authorities. In September 2019, the four ERDF MAs agreed to a common fraud policy.

Slovakia: The Government of the Slovak Republic approved a National Strategy for the Protection of the European Union's Financial Interests in the Slovak Republic in 2015, amended in 2019. This document provides a description of the individual parts of the antifraud cycle: prevention, detection, investigation and prosecution, and recovery of unduly paid amounts, and sanctions. It sets out general tasks to ensure that fraud risk management systems are put in place but does not contain specific procedures relating to FRM of ESI Funds.

Vlaanderen. There is no formal anti-fraud strategy at the federal level in Belgium, due to the separate operation and management of ESI funds by the regions (Vlaanderen, Wallonia, Brussels Capital Region). The Flanders policy statement outlines the definitions of fraud and conflict of interest, the institutional responsibilities between MA, CA, and AA, and outlines the procedures for reporting fraud. The aid granting authorities are responsible for their own individual anti-fraud measures and management. The Flemish ERDF anti-fraud policy specifies the division of roles between the different institutions. The policy promotes an 'ethical culture', in line with codes of conduct of the public service. Education/training, internal control systems and data analysis have received increased priority as active prevention tools, and detection, investigation, correction and prosecution measures are set out.

Most programme authorities consider that **fraud risk management has become a more strategic and integrated function of the programme and project management cycle** with a stronger emphasis on zero tolerance to fraud, a more proactive approach with robust procedures and increased capacity (e.g. CZ, Eng, FI, SK, Vla, Wal). For instance, in Finland fraud risk management has become a key function in its own right (rather than an element within the broader risk management procedures), and has become an increasingly important subject of discussion amongst policy makers. Similarly, the anti-fraud policy of the Flemish ERDF MA includes a more pro-active approach in 2014-20 structured around prevention, detection, correction and prosecution. Previously, there were no active anti-fraud measures with suspicions of potential fraud discovered ex post, e.g. during audit and control. For some countries, such as Slovakia, the current programming period marked the first steps in the development of an anti-fraud culture more generally with the approval of a National Strategy in 2015 (amended in 2019) introducing new procedures and methods that were improved over time and resulted in increased attention to fraud risk across authorities and implementation levels.

In practical terms, a key change compared to the 2007-2013 programming period is that **MAs were required to carry out fraud risk assessments** as part of the description of the management and control systems. In carrying out the fraud risk assessments, MAs/IBs used a Commission self-assessment tool tailored to specific contexts (discussed in the next section).

Institutional arrangements have been strengthened through the establishment of fraud risk management teams/working groups and increased capacity and training to develop more professionalised staff. In Slovakia, a Working Group was established tasked with activities related to the set-up, monitoring and evaluation of the FRM systems at the level of each OP including MAs and IB staff as well as other related bodies (e.g. Payment units, Certifying Authorities, National office of OLAF in the Slovak Republic). In England, awareness of fraud prevention and detection had always been incorporated into the programme management processes but there had not previously been dedicated teams to deal with fraud queries. The ERDF MA currently has two designated Counter Fraud Officers in place with a further two in training taking an accredited course. There are also lead officials responsible for counter fraud within each of the MA's six Growth Development Teams which are geographically distributed across the programme area.

Increased training on fraud risk management is also evident (FI, FR, Sco, Wal). In Finland, the training is offered at the MA level and via IBs to the project beneficiaries, while in France the focus has been on MAs. Fraud risk is now part of the training that all MA staff receive in Scotland, including a compulsory annual update. In Wales, several MA officials have completed accredited formal training in Investigative Practice provided by the Chartered Institute of Public Finance and Accountancy. On an ongoing basis, attendance at seminars and conferences by relevant staff are set as key objectives in their annual performance reviews. In addition, the Welsh Government's Head of Counter Fraud runs periodic training sessions for all MA staff to update and refresh their Counter Fraud awareness.

More central guidance on fraud risk management has been issued to facilitate the implementation of EU requirements (e.g. CZ, Eng, PT) along with internal management documents related to risk management procedures, responsibilities, internal manuals, codes of conduct/ethics detailing the procedures and rules related to the daily implementation of the fraud risk management systems. For instance, there has been far more guidance on countering fraud issued in England for 2014-20 than in previous periods, including distinct guidance for use within the ERDF MA itself, and guidance for grant recipients for setting up their own systems and processes. Importantly, the guidance provides a 'jumping off point' for conversations with recipients during the project appraisal process, which can have a preventative effect.

Cooperation among programme authorities related to fraud risk management has increased. In the Netherlands, the four MAs have agreed to share anonymised fraud cases during inter-MA coordination meetings for purposes of awareness creation and joint action. In Slovakia, the Central Coordination Body (CCB) does not have formal legal responsibilities for fraud risk management, but it has acquired an increased role through coordination of the OECD fact-finding mission in Slovakia during 2018-2019 and the informal consultation with the European Commission which followed.

There is also more extensive cooperation with institutions outside the programme implementation system responsible for combating and preventing crime (e.g. Police and the Public Prosecutor's Office) (PT, W-M). Warmińsko-Mazurskie established procedures for the exchange of information between the institutions of the ROP on proceedings conducted by law enforcement authorities and other authorised institutions against beneficiaries in order to use this information at the stage of project evaluation. In Portugal, a positive development is the strengthening of mechanisms of cooperation between the relevant fraud risk management entities (e.g. protocol between the ADC and the Public Prosecution Service).

The issue of conflict of interest has become more salient in fraud risk management approaches and procedures in 2014-20, particularly with respect to public procurement. For instance, in Warmińsko-Mazurskie, the MA / IBs were obliged to assess job positions where they identified tasks in which employees may be particularly vulnerable to risks of corrupt behaviour and conflicts of interest. More detailed and robust processes for addressing separation of duties have been introduced in Scotland for 2014-20 in response to audits.

Notwithstanding these positive trends, **effective and proportionate fraud risk management faces a number of important challenges**

- **The administrative burden** of complying with EU fraud risk management requirements is a commonly reported challenge among programme authorities. The work is considered laborious and disproportionate to the risk of fraud (AT, Biz, some regions in FI), adding to the complexity of management and control systems. Austria questions the value of the significant effort that goes into fraud risk management given that there has only been one fraudulent case identified in Austria in three programme periods. Also, a reasonable degree of risk is covered already by the procedures of the IBs, which in many cases have long-established, well-functioning systems. Similarly, proportionality is the key challenge for the Flemish MA. The programme is small, and the very few cases and irregularities lead to a low fraud risk. In some countries, such as Czechia, an overly formalistic approach was adopted by national authorities, which implied considerable administrative overload on implementing bodies. Similar gold-plating of EU rules with more onerous domestic requirements are also reported in Austria.

- **Interpretation of EU rules and guidance** on fraud risk management has been problematic for many MAs, especially where there is less experience in fraud risk management. For instance, some MAs interpreted EU requirements in broader terms and identified excessively long lists of fraud risks which were not operational or adequate during audit controls, and subsequently required amendments during implementation, the development of new risk catalogues and new assessment methods (SK). A lack of legal clarity in EU and national Czech law on conflict of interests has caused uncertainty for MA decision-making. There is also a lack of legislative clarity regarding final beneficiaries compounded by unreliable data on ownership in registers (CZ IROP).

- **Data checks, systems and registers** present operational challenges. In Scotland, the information that must be assessed by the MA to verify grant claims is complex, as they deal with a range of organisations and systems who keep records in very different ways, and have different ways of presenting information. The MA has an objective of training staff to spot potential issues and having the confidence to then challenge what they find. However, MAs may lack the necessary information to identify fraudulent

behaviour such as access to the sources of information available to investigative bodies, nor do they have the investigative powers of these bodies (for instance, cross-checking of information is difficult or impossible) (Pom). The utilisation and functioning of information systems relevant to fraud has been problematic in France. In Finland, the lack of a centralised State Aid register has made it difficult to check whether beneficiaries have received State Aid.

- **Methodological issues** have arisen in quantifying/scoring risk levels according to criteria, such as evaluation of the impact of the individual risks and the likelihood of their occurrence (SK). In this context, there is considered to be scope for improving the risk scoring tool designed by the Commission (W-M).

- **There is uneven implementation of fraud risk management.** In France, this is illustrated by the varied use of the ARACHNE system and implementation of anti-fraud measures. Similarly, it is difficult to ensure a consistent approach to risk assessment when implementation responsibilities are delegated to intermediate bodies at national and regional levels dealing with a diverse range of public and private and third sector beneficiaries (AT).

- **Limited national coordination can hinder a strategic and joined up approach**. In the Netherlands, the Dutch Court of Auditors recommends the establishment of a national anti-fraud strategy and improved coordination between payments to and expenditure from EU funds. The customs service (AFCOS) is coordinating anti-fraud measures for contributions to the EU and there is effectively no coordinator for subsidies from the EU in the Netherlands. The Court advises the designation of one responsible minister and one coordinating authority for EU payments, ideally combining this with coordination of contributions to the EU.[2] The absence of a centralised authority for fraud risk management can hamper coordination/exchange among MAs and the development of unified methodological guidance (SK). Under- reporting of fraudulent irregularities in France is partly attributed to weak coordination between central and regional authorities in fraud reporting.

- **Institutional cooperation and communication** between MAs with bodies related to law-enforcement may be suboptimal, and tensions can arise between different bodies in suspected fraud cases (MAs, AAs, PPO, etc.), such as where there is a lack of sufficient evidence to trigger an investigation by AMO or law-enforcement bodies (SK). Effective cooperation and coordination across institutions is therefore critical for fraud risk management (W-M). To address challenges of cooperation between the responsible bodies for anti-fraud, Greece has established a network including all MAs to provide a platform for constant cooperation.
- **Deficits in institutional capacity and shortages of skills** in fraud risk management, trainings and experts, can hamper fraud risk management tasks (FR, SK), especially tailoring EU fraud requirements to the specific context and needs of individual programmes (SK). To increase awareness of anti-fraud policy and measures in Greece, fraud risk management seminars have been organised for MAs and for beneficiaries by recognised experts. In other cases, there is capacity to organise training (e.g. on ARACHNE and other tools), but the human resources for periodic checks, formal meetings, or follow-up of each 'red flag' are lacking. One of the biggest issues in England is the large volume of projects involving procurement and many final beneficiaries that are at a stage removed from the MA, as they are not direct applicants to the programme. The challenge is to provide guidance and to build up capacity within the grant recipients to manage the process.

Lastly, it is important to note that **fraud risk management is a low priority in some countries** and not perceived to be particularly challenging, especially where fraud risks are considered to be minimal. For instance, fraud risk in Finland and Germany is low and therefore not seen to be a major priority for most MAs/IBs relative to other management tasks. In France, an independent report found that tackling fraud is not deemed a key priority by managing authorities which generally place much more onus on spending and operational delivery.

3.2 Fraud risk assessments

Fraud risk assessment is a core element of the 2014-20 regulatory framework to ensure that effective and proportionate anti-fraud measures are set up taking into account the risk identified. To support Member States in undertaking fraud risk assessments (FRA), the Commission developed guidance and a self-assessment tool in the form of a spreadsheet structured around four processes that are most prone to fraud risk:

- selection of applicants;
- implementation of projects by beneficiaries, focusing on procurement and labour costs;
- certification of costs and payments; and
- direct procurement process managed by the MA.

The guidance lists the most frequent fraud and corruption risks and sub-risks alongside an indicative assessment of the level of risk based on previous experiences, and potential mitigating control measures.

The FRA process is generally viewed positively especially in terms of raising awareness and encouraging discussion in MAs and IBs on fraud risks and the importance of promoting an anti-fraud culture with mitigation measures (FI, HR, SK, W-M). In Croatia, practical examples were elaborated that translated fraud indicators to real world scenarios to make it easier to understand the fraud risk indicators and detect fraudulent behaviour. The FRA is perceived to provide a useful way of institutionalising a systematic and consistent stock take of fraud risks in different priorities (DK, Eng, HR) supporting MAs in accelerating mitigation measures and enhancing the effectiveness of control systems (W-M). There are however questions about the need for a FRA exercise every year or two years, if there are no important changes with respect to the risks, the measures taken or suspected fraud cases reported (EL).

The Commission guidance was generally perceived to be useful, albeit complex and requiring simplification and tailoring to needs in many cases. The main difficulties reported were excessive detail and complexity (Eng, FI, Vla) e.g. requiring calculations of gross, net and residual risk rates (EL, FI) that are perceived to be somewhat formulaic and arbitrary (Vla). The strong emphasis on procurement and conflicts of interests was not always seen as relevant where MAs are not involved in procurement processes (Eng). The added value of the FRA has

been questioned in Austria. As an example, the Austrian Hotel and Tourism Bank IB already implements robust fraud risk prevention measures, but then had to also use the FRA template requiring additional and disproportionate effort. While there has been pressure to make use of this tool, in practice it is not considered necessary for all IBs in Austria.

There are mixed views on the substantive impact of the FRA on procedures and approaches. In some cases the assessment did not lead to changes in the management and control system – or only minor changes – which were already deemed to be effective (AT, Pom, SK). Given that most fraud issues are likely to arise during the implementation of contracted projects, it is the effectiveness of detection measures (e.g. checks or whistleblowing) that is most critical for reducing instances of fraud (NL, Wal). However, the follow-up of fraud risk assessment recommendations can lead to concrete changes in procedures, measures and priority (e.g. EL, PT, Vla). For instance, conflicts of interest were singled out as having led to the introduction of new measures in Greece. Similarly, in Vlaanderen, the assessment led to extra attention to the declaration of impartiality and independence, applicable to personnel responsible for selection and control. In the Netherlands, the challenges/risks identified in the 2019 FRA led to the establishment of an integrity policy in every MA, which extends to the regional OP partners (i.e. provinces and municipalities in the programme).

The main suggestions put forward to improve fraud risk assessments are as follows.

Coordination, integration and cooperation. Greater harmonisation and coordination should be pursued with regards to IT systems and fraud-related data, information sharing, inter-institutional relations, as well as methodological guidance.

- **Data systems.** Connectivity between the data stored in different IT systems needs to be improved and mechanisms for centralised access to data developed (e.g. a central register of identified fraudulent practices) (e.g. CZ, FI, HR, NL, PT, SK). Improving the interconnectivity of ARACHNE with other databases and ensuring more rapid data exchange is important in this regard (e.g. CZ, NL, SK; see also Section 6.3). Integration of data in various existing IT systems and registers could help to improve data management and verification, and decrease the burden on staff consulting a wide range on disconnected systems. Some steps in this direction have already been taken e.g. in Finland, where the new data monitoring system, Eura 2021, will have new links for example to business registers, which is expected to improve data access, although there is scope for further improvements.

- **Information exchange and inter-institutional cooperation**. There is need for opportunities and mechanisms for exchanging knowledge, experience and information, including through the enhancement of cooperation between different bodies and stakeholders involved in fraud risk management (e.g. CZ, HR, Pom, SK, W-M). Rapid and efficient exchange of information could be facilitated, for instance, through enhanced cooperation with investigative and law enforcement authorities on fraud cases (SK) or access to the MA to recent, anonymised fraud cases (Pom); as well as participation in the risk assessment of relevant entities involved in combating and tackling fraud (W-M).

- **Methodological coordination**. There is a need for greater methodological uniformity and coordination in some cases e.g. the majority of the MAs in Slovakia consider that FRA and fraud risk management in general could be improved through the introduction of an overarching and uniform methodological framework of risk management or overseeing body that could guide the MAs in the process at national level.

Simplification and proportionality. Simplification of FRA could help to improve the proportionality of the exercise and increase its value for programme authorities. This could apply to the scoring tool / system (e.g. AT, EL, W-M), e.g. by focusing on scoring the net risk only (without scoring gross risk or individual measures), so as to give emphasis to the measures themselves as well as to how they mitigate the fraud risk and whether an action plan is required. The need for more proportionality is also important for the Austrian and Finnish authorities (Tampere), e.g. by relying on domestic risk assessments/tools if they are used and are effective.

Awareness raising, capacity-building and information provision. Fraud risk assessment can be improved by raising the awareness of fraud situations, e.g. by organising educational workshops (HR) or fraud awareness campaigns at EU level that would enable institutions, beneficiaries and potential beneficiaries to understand the importance of fraud prevention (W-M). Targeted training programmes could help improve skills and increase the capacity to perform FRA (e.g. SK). Improving the availability of and acces to relevant information is also important. For instance there is need to promote the exchange of knowledge and sharing of good practices on how to efficiently use ARACHNE, e.g. via specialised workshops and the production of a handbook of good practices (CZ IROP). Wider publication and updating of information on the results of OLAF auditors' and MA controllers' work is also viewed as desirable for the purposes of risk assessment (W-M). In particular, there is interest in the provision by OLAF of information on the number of fraud cases detected every quarter and the associated amount; the industries most affected by fraud; the most common fraud practices.

Further suggested improvements include:

1. **A greater focus on preventative fraud work** as opposed to control mechanisms (FI).

2. **Ongoing assessment of fraud risks.** FRA can be improved by continuously (i) updating a catalogue of risk types with the aim of foreseeing all risk types as well as following measures to mitigate them, and (ii) assessing the effectiveness of the current controls regarding fraud risk, in order to improve control system and to reduce possible risks (e.g. HR).

3. **Ensuring the independence of FRA**. According to the Danish MA, carrying out fraud risk assessment by an independent external actor might strengthen the external credibility of the assessment. However, the lack of insight into the day-to-day practices could potentially compromise the exercise.

4. **Further development of risk indicators** for each of the risks in the FRA database, which could help enhance detection of fraud risks (FI).

5. **More objective risk scoring.** According to the Greek authorities, the current emphasis is more on qualitative scoring of risk, which is somewhat subjective and reliant on the view of individual assessors (EL).

6. **Using statistical data and techniques to determine the probability of the fraud risk** from all findings of suspected fraudulent cases identified in controls, or by AA and other bodies (e.g. SK). Several additional techniques have been identified (SK): Event Tree Analysis, Hazard and Operability Study, Preliminary Hazard Analysis, What if methodology, SWOT analysis, impact analysis. Most IQ-Net programme authorities do not use such methods/tools and mainly rely on the FRA tool on the basis of expert assessment (e.g. AT, CZ IROP, EL, NL, PT), ARACHNE and other similar databases (e.g. Wal).

3.3 Managing conflicts of interest

The management of conflicts of interest is an increasingly important component of ESIF fraud risk management. Conflicts of interest can arise in a range of situations – especially with respect to public procurement of works, supplies and services – and require appropriate management processes to prevent impartial and objective decision-making being compromised. The regulation of conflicts of interest in ESIF in 2014-20 is governed by the EU's Financial Regulation of 2012 revised in 2018. These rules oblige actors involved in the implementation, management, audit and control of EU funding to refrain from taking any action that may bring their own interests into conflict with those of the EU. The EU Financial Regulation (Art.61) defines conflicts of interest in the spending and management of EU funding as existing

> ***"where the impartial and objective exercise of the functions of a financial actor or other person…is compromised for reasons involving family, emotional life, political or national affinity, economic interest or any other shared interest with a recipient."***

A revised concept of conflict of interests was introduced in the EU's Financial Regulation in 2018. The main changes introduced in Article 61 were: a re-worded definition of conflict of interest covering "any other direct or indirect personal interest", more situations covered which may "objectively be perceived as a conflict of interests", and broader scope including explicit application to ESIF requiring national authorities to avoid and manage conflicts of interest. Member States are required to:

1) establish internal control systems including avoidance of conflict of interest, and audit these systems;

2) establish prevention measures (e.g. declaration of absence of conflict, assets disclosure); and

3) establish whether a conflict exists in a given case and apply corresponding mitigation measures.

IQ-Net partners apply these obligations through **direct application of EU rules and national legislation.** For instance, in Finland the Administrative Procedure Act requires avoiding conflicts of interest in the administration and provides details on how to act in the event of a conflict of interest e.g. disclosure of conflict in advance of procurement. In Portugal, national legislation takes as a reference point the definitions adopted in the EU Financial Regulation and various domestic legal norms are published in line with EU legislation stipulating that any situation of conflict of interest must be declared. While the measures for mitigating conflict of interest are not new, they have grown in importance. In Slovakia, several legislative acts have been adopted. In particular, in accordance with the Civil Service Act, civil service employees are obliged to refrain from actions that could lead to a conflict of interest between their public responsibilities and their personal interests, and in particular to refrain from misusing information obtained in connection with public service for own benefit or for the benefit of another.

The absence of clear and binding provisions in EU and national legislation can leave scope for interpretation which can be problematic for ESIF management. For instance in Czechia, the national legislation transposing the EU Financial Regulation does not specify in any accompanying interpretative legislation how to apply Article 61 in practice, namely what "appropriate measures" should be used, how relationships of family members should be addressed etc. In this context, a solution could be for the EU to develop handbooks/manuals to clarify interpretation problems for MAs and other authorities.

More detailed guidance on conflicts of interest is published tailored to ESIF management and implementation arrangements to raise awareness on the risks and procedures to follow. Illustrative examples of comprehensive guidance include:

England: The ERDF MA published guidance on identifying, managing and monitoring conflicts of interest in ERDF, focused primarily on decisions on the allocation of funding by the MA and IBs, and procurement by grant recipients, including non-contracting authorities. There is a separate conflicts of interest statement of requirements for IBs. Practical examples of conflicts of interest and how they can be managed are provided in the guidance (Box 1).

Slovakia: The Central Coordination Body also prepared methodological guidance on how to determine conflict of interest in public procurement, and an additional guideline from OLAF is provided to employees. A specific document has also been adopted by the CBB, with instructions on the use of the ARACHNE data analysis tool, among others, for the purpose of identifying conflicts of interest.

Conflicts of interest are minimised by the establishment of **management and control systems based on a clear division of competences in the organisational structures** of MAs/IBs through the principle of a separation of key functions and job tasks. For instance, the Dutch West MA system ensures that technical and financial assessments of projects are undertaken by different staff ensuring a separation of functions, and by having an expert committee (per

ERDF region) and 'urban advisory group' (advising on projects in the urban ITIs) that are independent. Prior to meetings of the expert committee and the urban advisory group, voting members are asked to declare potential conflicts of interest and. If there is, they will then leave the room for the substantive assessment of that project.

The use of declarations of absence of conflict of interest is common practice.

Austria: all members of staff sign a declaration of absence of conflict of interest when taking their post. This is also the case in IBs, many of which are departments of *Land* Governments, which have their own rules.

Finland: declarations of absence of conflict of interest were adopted following the updated financial regulation of 2018, adapted to the practices of the MA, the IBs and also recommended to be used by the beneficiaries. The adoption of the declaration was viewed as straightforward by the MA with no negative implications i.e. in terms of increasing administrative burden or mistrust.

Greece: the Partnership Agreement and a national law oblige MA staff and external experts to provide a declaration of absence of conflict of interest. In MAs, the descriptions of the post of Head of the MA, heads of Units, staff responsible for the selection, the verifications entail an obligation for declaration of absence of conflict of interest.

Programme authorities tend to mainly rely on the declarations of the beneficiary and people involved in the grant awarding process when assessing conflicts of interest. **They also undertake controls, or checks** of information in the declarations against other sources such as company data registers (DK, HR, PT, SK, Vla, Wales, W-M). If fraud risk-related information about an applicant, beneficiary or third party is received, investigations/controls are undertaken and competent bodies are informed e.g. IBs, fraud units and, if necessary, competent law enforcement authorities (CZ, DK, HR, PT, SK, Vla). The information is recorded on IT systems / red flag registers, and financial corrections are applied if conflicts are proven.

With respect to public procurement, declarations and controls are also the main tools used to identify conflicts of interest. As noted, members of evaluation committees sign a conflict of interest Declaration Form, which in some cases is checked against information in registers (DK, SK, Vla). In the event of a conflict, the member is not permitted to play any role in the procurement. If, due to exceptional circumstances, it is not possible to exclude this person, grant recipients should ensure the decision taken is fully transparent and based on transparent and fair evidence (Eng). Reporting of undeclared conflicts lead to all stages of the procurement process being repeated. When conflicts of interest are detected during financial controls, the MA/IB will requests checks by the Public Procurement Office and may conduct on-the-spot checks (SK). In some cases, the MA and staff have recourse to an Ethics Team, whose task is to provide advice to employees in ethically doubtful situations (W-M).

Box 1: Examples of conflicts of interest and how they can be managed – extract from England ERDF MA guidance

Recommendations by ESIF Committees

Example problem: An individual (Person A) owns a business which provides paid consultancy advice to organisations looking to submit bids for the ERDF/ESF.

Person A also sits on an ESIF Committee which provides recommendations to the MA in relation to the drafting of calls for funding and the selection of projects for funding under the ERDF/ESF. An organisation that PersonA's consultancy business has recently advised,applies for funding. Person A has a conflict of interest between their role advising an applicant for funding and their role sitting on the ESIF Committee assessing this application.

Solution: These types of conflicts can be quite common but can be easily managed by parties declaring their interests and, where necessary, absenting themselves in order to avoid any bias in decision making.

Decision making by Intermediate Bodies

Example problem: A member of staff working in an Intermediate Body (Person B) is responsible for managing an ERDF/ESF funded Project where a close relative/ friend is employed in a senior position. A recent monitoring visit identifies a number of irregularities which results in the applicationof a significant financial penalty to the Project. Rather than process the irregularities in line with the Department's guidance on corrections, Person B sets about exerting undue pressure on the monitoring team to remove their finding of irregularities and fails to provide any evidence to support their removal.

Solution: The correct process would be for Person B to deal with the irregularities in line with the Department's guidance on corrections. However, Person B allows their close relationship with the Project to interfere with this process which results in biased decision making.

Note: This example relates to an agreed irregularity and does not remove the Project's right to challenge the initial findings of the monitoring team by providing further evidence through a contradictory process.

Procurement by grant recipients

Example problem: An organisation (the Grant Recipient) is awarded ERDF/ESF to construct a business centre; the director of the Grant Recipient is also a director of a construction company(Company A). The Grant Recipient appoints an independent Agent to carry out the procurement process, removing the Grant Recipient from any involvement in the decision making process.

The Grant Recipient later makes a request that the Agent considers including Company A in the procurement process. Company A eventually wins the contract. The Grant Recipient's direct involvement in the procurement process by asking the Agent to consider including Company A suggests a potential conflict of interest.

Solution: Whether there is a conflictof interest depends upon how this request was managed. If the independent Agent assessed Company A to fit the criteria for inclusion in the procurement process and steps were taken to ensure that the potential conflict was appropriately managed, no irregularity for actual conflict of interest will be identified. If, however, Company A did not fit the criteria, or the potential conflict was not appropriately managed, an irregularity is likely to be identified.

Source: HM Government (2019) Guidance on Identifying, Managing and Monitoring Conflicts of Interest within ERDF and ESF; https://bit.ly/3lc4z7W

3.4 Institutional coordination

The institutional responsibility for fraud risk management lies with the Managing Authorities and other related bodies such as Intermediate Bodies responsible for the implementation of the OPs. However, central Anti-Fraud Coordination Services (AFCOS) and other coordinating bodies also play a role in many countries. Typical examples of institutional arrangements include the following.

In **Austria**, there is a dedicated risk manager at the MA (ÖROK) and four 'risk owners', one for each of the four areas of risk identified in the risk strategy, fraud being one of them. Each IB has a dedicated risk manager, too, which regularly reports to the risk manager at the MA. Many of the larger IBs that are running major domestic funding programmes also have an elaborate risk management system in place. Fraud risk is one of four types of risk addressed in the risk strategy. The MA is predominantly covering the programme-wide risks (structural, organisational, operational), while IBs are predominantly looking at fraud risk.

In **Finland**, this fraud risk management responsibility rests with the MA (the Ministry of Economic Affairs and Employment) and other authorities responsible for the implementation of the OP (e.g. 18 Regional Councils, 15 Centres for Economic Development, Transport and the Environment (ELY), which are deconcentrated offices of the central State administration, and specifically the four coordinating Regional Councils and the four specialist ELY-centres which specialise in ESIF management in 2014-20).

In **Greece**, the key responsibility for fraud risk management lies with Managing Authorities. The legal framework (Art. 52 of Law 4314/2014) provides, *inter alia*, for the establishment of a team in each MA, whose task is to assess fraud risks, propose and implement any corrective measures and report the results to the Internal Network. The Special Service for Institutional Support (EYTHY) is responsible for the design and monitoring of the management and control systems and formulating the national anti-fraud strategy for Structural Funds.

Strong coordination, cooperation and information exchange on fraud management is reported in a number of cases (e.g. DK, EL, Eng, FI, PT), facilitated by factors such as:

- **a clear division of competences** assigned to the relevant bodies in the management and control systems as well as the relevant national and EU legislative obligations;
- **a culture of openness and cooperation** between public authorities due to the institutional set-up e.g. in Denmark, the MA, payment and auditing authorities, although separate entities, are all part of the Danish Business Authority; and
- **the limited scale of funding and size of the institutions** involved in fraud management e.g. in Finland, the fact that the MA, AA and CA are relatively small bodies facilitates cooperation on an ongoing basis.

Coordination is achieved through a range of formal and informal institutional arrangements and channels for interaction and information exchange, including the following.

i Cooperation within the management and control systems

Formal and informal cooperation on fraud management is pursued within the existing ESIF management structures and MCSs, including through coordination between the MAs, IBs, AAs, CAs and other relevant bodies. This is facilitated through established and dedicated cooperation channels and platforms, harmonisation of methodologies and procedures across MAs, information exchange via IT systems or reporting mechanisms.

Exchange between MAs is ensured via regular meetings, common use of information systems and guidance, joint fraud risk assessment exercises, or exchange of good practices. In the UK, for example, the MAs meet to discuss best practices implemented and lessons learned in individual programme areas. In the Netherlands, the ERDF MAs coordinate their anti-fraud efforts by undertaking the FRA jointly and exchanging good practices. Every two years, the Ministry of Finance chairs the FRA meetings with the other MAs and the CA, and reports on development during annual inter-MA meetings. In Austria, there is a regular exchange between the MA and IBs every 2-3 months, covering all programme implementation issues, including management and fraud risks.

Active interaction with other bodies in the MCS is also pursued. For instance in Finland, the MA, AA and the CA work closely together and exchange information on a regular basis. In Croatia, the collaboration of the OPCC bodies with SCIF and AFCOS is envisaged in the common national framework for risk management, and annual risk assessment of all bodies of the MCS of the OPCC is shared with the SCIF office as a coordinating service for irregularities and fraud. In Greece, the coordination and cooperation between competent authorities is provided for in the relevant procedures and protocols of management and control system which are common for all MAs.

Cooperation on fraud management within the existing MCSs is facilitated by the following.

- **Common use and exchange of data via IT systems.** For example, in the Netherlands, all ERDF MAs use the same company register/database (Company Info). In Poland, all MAs use IMS-Signals, a database for sharing data on suspected fraud cases, through which they exchange information about red flags. In Portugal, all the MAs have access to the historical data on ESIF beneficiaries, which is centralised in the Agency for Development and Cohesion (see Box 2).

Box 2: Identifying and sharing information on fraud indicators in Portugal

In Portugal, the principle of *idoneidade* (lit. 'reputability', 'trustworthiness') is enshrined in national legislation, which is based on the historical data of beneficiaries' interaction with the ESIF and reflected in conditions ruling the access to the Structural Funds (*código de idoneidade*).

These data on entities that have benefited from ESIF support since 1986 include, *inter alia*, information related to any past irregularities in the use of the Funds (e.g. administrative or financial irregularities, irregularities related to audits etc.). Based on these data, an entity may be entitled to or prohibited from future support.

The data are stored and treated internally (centralised at the level of ADC) and are available not only to all organic units of the ADC, but also the MAs. It is taken into account at the application and project appraisal stage and when making payments (upon verifying absence of any situation of risk). It can provide an indication of a potential fraud risk associated with a beneficiary and signal to the MA the appropriate course of action with regards to the respective application (e.g. if closer monitoring or inhibition from accessing funds is required).

The *código de idoneidade* is also consulted when a complaint is received regarding a specific entity. Such cases are investigated by the Public Prosecution Service, which can make a judgement on the probability of non-fulfilment by the entity in question, with consequences for support provision. I.e. this helps ensure that the amounts to be paid are only guaranteed from the moment when it has been established that the expense is not subject to any (potential) irregularity. This is a useful prevention mechanism that can help avoid future situations of fraud in the use of Funds.

Source: IQ-Net fieldwork

- **Harmonised or shared methodologies and procedures across MAs** (e.g. EL, ES, HR, PT, SK). For example in Spain, at the start of the period, the central MA in coordination with the AA and AFCOS required all regions to align their methodologies in conducting their Fraud Risk Assessment, to tailor mitigating measures proposed by the Commission to their specific context, and to document the methodology and anti-fraud measures in an annex to their MCS description manuals.[3] Similarly in Portugal, a single legislative norm was issued,[4] which provides guidance to the different MAs for the implementation of the anti-fraud strategy as well as for carrying out a fraud risk assessment. This norm aims to systematise the requirements that the MAs are recommended to implement in terms of effective and proportionate anti-fraud measures, and to harmonise the procedures by the different MAs. In Slovakia, despite the absence of a single methodological guidance, MAs and IBs exchange information on their methodologies for risk assessment, as well as controls mechanisms and results of performed system audits through informal meetings or other channels.

- **Information shared via mechanisms for reporting/complaints**. In Greece and Portugal, information is exchanged among the relevant bodies through internal reporting systems or mechanisms for reception and examination of complaints.

- **Specific cooperation agreements** between relevant bodies, such as cooperation protocols (e.g. between the Portuguese coordination authority ADC and the Public Prosecution Service) or agreements on cooperation and exchange of information (e.g. between Ministry of Finance[5] and Local Contact Points AFCOS / MAs in CZ).

- **Informal information exchange**. For instance in Vlaanderen, due to the small size of the teams and departments, informal exchange happens more frequently and on an ad hoc basis. In Slovakia, most exchange of information and experiences is also performed on an informal basis, although an official platform for exchange would be welcomed.

- **Allocation of contact points for anti-fraud measures**. Contact persons appointed for cooperation in the field of fraud (e.g. AT, FI, W-M) improve the flow of information in and between the relevant entities. For instance in both Austria and Finland, there are responsible contact persons at the IBs, facilitating dissemination of information. Contact points for AFCOS (e.g. CZ) and OLAF (e.g. HR) have also been established.

ii Coordinating bodies / AFCOS

Central coordinating authorities dedicated to tackling fraud and strengthening transparency, integrity and accountability of government more widely have been established in many countries. These **include the Anti-Fraud Coordination Services (AFCOS), national AFCOS networks as well as other coordinating bodies**.

The set-up and functions of AFCOS differ across IQ-Net countries. In some cases, AFCOS functions are performed by a single authority – examples include the Inspectorate-General of Finance[6] as the Audit Authority in Portugal; the internal financial control office for the national public sector and Audit Authority in Spain (see Box 4); or the Ministry of Finance as the Central Contact Point for coordinating services for cooperation with OLAF in Czechia. AFCOS bodies tend to be under the responsibility of a Ministry of Finance (See Table 3).

Table 3: AFCOS in IQ-Net Member States

Member State	Name of the authority	Relevant administration
Austria	Department for Anti-fraud, Tax and Customs	Ministry of Finance
Belgium	Interdepartment Commission for Coordination of the Fight against Fraud (CICF / ICCF)	Ministry of Economy
Croatia	Service for Combating Irregularities and Fraud - Directorate for Financial Management, Internal Audit and Supervision	Ministry of Finance
Czech Republic	Department 69 - "Analysis and Reporting Irregularities"	Ministry of Finance
Denmark	7th Division – Environment, food, climate, energy and EU Budget	Ministry of Finance
Finland	Government Financial Controller	Ministry of Finance
France	Mission Interministérielle de Coordination Anti Fraude (MICAF)	Ministry of Finance
Germany	Division for the protection of EU financial interests	Ministry of Finance
Greece	National Transparency Authority (NTA)	National Transparency Authority (NTA)
Netherlands	Customs Information Centre	Ministry of Finance
Poland	Department for Audit of Public Funds	Ministry of Finance
Portugal	General Finance Inspectorate	Ministry of Finance
Slovak Republic	Control and Anti-Corruption Section	Government Office of the Slovak Republic
Spain	General State Inspection	Ministry of Finance
Sweden	Swedish Economic Crime Authority	Ministry of Justice

Source: European Commission European Anti-Fraud Office (OLAF)

Greece has set up an independent National Transparency Authority as its AFCOS to ensure a more coordinated approach by centralising the functions scattered across a range of bodies with anti-corruption roles (Box 3).

Box 3: Greek National Transparency Authority

In Greece, at national level, the central Authority dedicated to strengthening transparency, integrity and accountability of government is the National Transparency Authority (NTA), which has been established under Art. 82 of Law 4622/2019 (FEK A 133). NTA is also designated as the Greek Anti-Fraud Coordination Service (AFCOs) according to Regulation (EU, Euratom) 883/2013 in collaboration with the Financial and Economic Crime Unit (SDOE) of the Ministry of Finance. As AFCOS, the NTA:

- coordinates national competent authorities/bodies for combating fraud;
- cooperates with the relevant EC bodies, principally OLAF;
- submits the questionnaire on the application of Article 325 of the Treaty on the Functioning of the EU (TFEU);
- receives complaints about cases concerning the co-financed, transnational and other programmes;
- removes conflicts and resolve issues of overlapping responsibilities between agencies or bodies involved in combating corruption and fraud.

Source: IQ-Net fieldwork

Box 4: Spanish central Anti-Fraud Coordination Service

In Spain, the central Anti-Fraud Coordination Service (AFCOS) responsible for fraud risk management (*El Servicio Nacional de Coordinación Antifraude*) was created as an entity under the responsibility of the internal financial control office for the national public sector (*IGAE Intervención General de la Administración del Estado*), which is also the Audit Authority for ESIF. The SNCA was created in 2014 in response to EU regulatory requriements on fraud risk management and coordination with OLAF (Reg 883/2013). It is resposible for:

- leading the creation and implementation of national strategies and promoting legislative and administrative changes necessary to protect the financial interests of the EU;
- identifying possible deficiencies in the national systems for the management of EU funds;
- establishing the channels of coordination and information on irregularities and suspected fraud between the different national institutions and OLAF;
- promoting training for the prevention and fight against fraud.

The national central MA is responsible for coordination and interaction with the regions on management (including fraud) and with the Commission, but each Intermediate Body is responsible for implementing the fraud management procedures and controls to detect and prevent fraud within its region and to report findings.

Source: IQ-Net fieldwork

Wider AFCOS networks, encompassing a wide range of relevant entities and actors, **have been established** in some cases. For instance:

Croatia - the AFCOS system includes: a network of bodies included in management and control system; a network of bodies dealing with the fight against fraud, corruption or any other form of irregularity in the system;[7] and the Ministry of Finance – Department for Combating Irregularities and Fraud. MAs continuously cooperates

with AFCOS network and the Agency for the Audit of the EU Programme Implementation System.

Denmark - the national AFCOS network comprises the Danish Agricultural Agency, the Danish Fishery Agency, the Danish Customs Agency, the Danish Police and the Danish Business Authority. The Danish authorities meet regularly through this network to exchange experiences, e.g. on the management of concrete fraud cases.

Apart from AFCOS or where AFCOS are not established (e.g. BE), **coordinating functions may be performed by other entities**. Some examples include:

Greece - the Special Service for Institutional Support (EYTHY), functioning as the central Authority for structural actions, exchanges information with all MAs regarding fraud risk assessment results and corrective or proposed measures, and examines whether there is a need to adapt further measures to the Management and Control System, issue instructions or proposals at national level.

Belgium - at federal level, the Interdepartmental Commission for the Coordination of Fraud (ICCF) provides a space for informal exchange of information and discussion of FRA checklists. Although the regions are not officially represented, the regional and EC representatives of the ESIF are invited to the meetings.

Croatia - the Department for Combating Irregularities and Fraud (Ministry of Finance) performs a coordinating role for irregularities and fraud within the system and forms a contact point for OLAF.

iii Cooperation networks

Coordination and information exchange on fraud-related issues are also pursued via networks, such as for instance:

Internal Antifraud Network in Greece, which operates between all MAs and under the coordination of EYTHY and via which the exchange of information on the results of fraud risk management, corrective measures, best practices and lessons learnt is ensured.

Irregularity Management Network and networks of coordinators in the field of public procurement and state aid in Croatia, in which representatives of all bodies of the MCS participate. Regular meetings of these networks allow to share good practices and recommendations in order to prevent irregularities arising from the misapplication of rules related to state aid and public procurement.

iv Dedicated working groups / think tanks

Working groups on fraud-related issues have been created across a number of countries / regions, facilitating cooperation and information exchange. Some examples include:

Finland - a new working group of fraud prevention is planned to be established for the authorities of the different EU funds which brings together representatives of the key Ministries.

Czechia - meetings of the Working Group Control, Audit, Irregularities (PS KAN) under the auspices of the Ministry of Finance are held regularly.

Warmińsko-Mazurskie - information exchange is facilitated via the working groups of the Inter-ministerial Team for Combating Financial Irregularities Against Poland.

Croatia - MCS body representatives are regularly invited to Anti-fraud group meeting and working groups to share experience and information on fraud risks and make recommendations for improvement.

Slovakia - the establishment of a Working Group or a Working Party tasked with activities related to the set-up, monitoring and evaluation of the FRM systems at the level of each OP and in most cases open for external entities is seen as a facilitator of cooperation.

Coordination and information exchange are also ensured through **joint analytical work.** For instance in Portugal, a Think Tank was created to identify areas of high fraud risk and response measures as well as opportunities for improving cooperation between the various entities involved in fraud risk management (see Box 5).

Box 5: Anti-fraud Think Tank in Portugal

In Portugal, a Think Tank was created in August 2020 at the initiative of the Public Prosecution Service, with the participation of representatives of national bodies involved in the coordination and auditing of European funds. The aim is to identify: (i) areas of high risk of fraudulent behaviour; (ii) fraud prevention guidelines in the management and control of European funds; (iii) action methodologies / strategies adjusted to the identified fraudulent behaviour, to prevent and combat fraud in European funds; and (iv) opportunities for improving cooperation between relevant entities.

The group comprises the Public Prosecution Service, the Judiciary Police, the Inspectorate-General of Finance (AA/AFCOS), OLAF, the National Court of Auditors, the ADC, and representatives of civil and academic society in the area of public policies and the fight against fraud.

The Think Tank will have an expected duration of two years and is anticipated to produce recommendations relevant for the next programming period.

Source: IQ-Net fieldwork

v Other exchange platforms

Other channels and platforms for information sharing and cooperation include joint conferences, workshops, seminars and consultations on fraud-related issues. For instance:

Netherlands - the Ministry of Finance brings the various parties together as part of **national anti-fraud consultations**. The outcome of the FRA is also discussed and determined in **various meeting structures**. The AA also participates in these meetings, and requires the MAs to fill in an annual checklist on fraud risks. The 2019 meeting with all Dutch anti-fraud actors has strengthened inter-governmental cooperation, although has not received a clear follow-up yet.

Czechia - the Central Contact Point for cooperation with OLAF organises **seminars** at least twice a year for its national partners (Local Contact Points AFCOS, the Police

of the Czech Republic, the General Directorate of Customs, the General Financial Directorate, the Supreme Public Prosecutor's Office, the Supreme Audit Office, etc.).

United Kingdom - the MAs participate in **meetings** where best practices and lessons learned in individual programme areas are discussed. In Wales, MA staff have attended several **conferences** alongside colleagues within the AA.

vi Cooperation with investigative / prosecution bodies

Such cooperation and information exchange are pursued via the existing distribution of responsibilities within the national institutional system as well as dedicated channels such as cooperation protocols, seminars and working groups, among others. For example:

Nordrhein-Westfalen - MA/AA/IBs identify fraud risks and detect suspicious cases, which are then automatically referred to prosecution bodies for investigation.

Warmińsko-Mazurskie - MA and IB representatives participate in working groups and exchange of information between government administration bodies, control bodies, police and prosecutors' offices.

Czechia - seminars organised by the Central Contact Point for cooperation with OLAF involve the Supreme Public Prosecutor's Office and the Police of the Czech Republic, among others.

Portugal - common solutions and coordination have been developed with national investigative bodies, including the Public Prosecution Service, reinforced via e.g. cooperation protocols (see Box 6).

Box 6: Cooperation with investigative bodies in Portugal

In Portugal, coordination is ensured with national investigative bodies, including the Public Prosecution Service (*Ministério Público*) and its bodies (including Attorney General's Office and Central Department of Investigation and Penal Action, DCIAP).

In 2019, a collaboration protocol was signed between the DCIAP (as a coordinating and directing body for the investigation and prevention of violent crime and within the scope of its functions of coordinating fraud which jeopardises the EU's financial interests) and the ADC (responsible for coordinating the regional development policy co-financed by EU Funds). It aims to support implementation of mechanisms for technical cooperation, via exchange of knowledge and information related to ESIF-supported projects, applicants and beneficiaries, as well as to increase mutual coordination. This Protocol formalises the already exisitng cooperation with the Public Prosecution Service.

Source: IQ-Net fieldwork and http://dciap.ministeriopublico.pt/pagina/protocolo-de-colaboracao-entre-dciap-e-adc-ip

vii Joint training actions

Coordination is also pursued through joint training activities and events. For instance in France, there are several training actions promoted amongst the different bodies responsible for audit. This is done in cooperation between DNLF/MICAF, CICC (the national audit authority) and the association of French regions, and made available to several national and regional

administrations. In Finland, the coordination between the MA and the IBs takes place through the training events, where the MA disseminates information to the IBs.

There is scope for improving coordination/cooperation on fraud management to ensure a more systematic approach (e.g. AT, CZ, SK). For instance in Austria, there are only informal contacts between the MA/AA and other bodies; similarly in Vlaanderen, there is very limited cooperation with the AA and with the Flemish ESF OP, and even less with the Walloon authorities. In both Slovakia and Czechia, cooperation is limited although seen as desirable. In Slovakia, structured coordination on fraud management between MAs and other related bodies is limited, reflected in a lack of uniform methodological practices and inconsistencies in audit findings produced by the AAs.[8] The issues stressed by the Czech IROP include lack of cooperation that is beneficial for implementation practice, including specific cases and court decisions; time to share experiences within the Working Group on Controls and Irregularities; lack of central fraud risk management/guidance documents to regulate/coordinate fraud risk practices; and the fact that cooperation is not systematic and only takes place on informal basis between MAs.

Suggestions for improving cooperation included the following:

- establishment of a single **coordinating authority** - the Dutch national Court of Audit concluded in May 2020 that the organisation of anti-fraud measures and fraud reporting could be strengthened by establishing one coordinating authority;
- provision of a **single methodological guidance** on FRM (SK);
- creation of an official, **coordinated platform for information exchange** and advice sharing (SK);[9] and
- **enhancing cooperation with law-enforcement and prosecution bodies -** the Slovak Central Coordination Body sees benefits in such cooperation, in the form of regular thematic presentations from the Prosecutor's Office on actual fraud related cases that are being/were investigated.

4 FRAUD RISK MANAGEMENT EFFECTIVENESS AND PROPORTIONALITY

4.1 Effectiveness

To assess the perceived effectiveness of anti-fraud measures in Cohesion Policy, a survey was undertaken of 29 managing and programme authorities represented by IQ-Net members. Following the approach used by the ECA Special Report 'Tackling fraud in EU Cohesion spending', a distinction was made between fraud prevention measures and fraud detection measures. The respondents were first asked whether each measure was used and then to provide a rating score of the perceived effectiveness of the measure on a scale of 0-10.

The most frequently used **prevention measures**, by over 90 percent of respondents, were

- Anti-fraud training for staff
- Formal policy on conflicts of interest
- Adoption of a code of conduct for employees
- Fraud risk-awareness measures for applicants/beneficiaries
- Fraud risk-awareness measurers for management bodies

Table 4: Fraud prevention measures implemented by IQ-net authorities and their perceived effectiveness

Prevention measures	Usage (%)	Effectiveness Rating (0-10)
Formal policy on conflicts of interest	93.1	8.0
Adoption of a code of conduct for employees	93.1	8.0
Fraud risk-awareness measures for management bodies	92.6	8.0
Publication of anti-fraud policy	84.6	7.9
Anti-fraud training for staff	93.1	7.7
Support programmes for employees exposed to fraud	29.2	7.5
Fraud risk-awareness measures for applicants/beneficiaries	92.3	7.3
Background checks on employees	56.0	6.4
Reward / Bounty schemes for whistleblowers	16.7	5.6

Source: EPRC survey of IQ-Net members

The least used prevention measures are Reward / Bounty schemes for whistle-blowers (17 percent), support programmes for employees exposed to fraud (29 percent) and background checks on employees (56 percent).

In terms of effectiveness, the prevention measures perceived to be most effective are a formal policy on conflicts of interest, a code of conduct for employees, and fraud risk-awareness measurers for management bodies – all with an average perceived effectiveness rating of 8

out of 10. More than two thirds of the prevention measures have a perceived effectiveness rating of 7 or more out of 10.

At the other end of the spectrum, the measures that are perceived to be the least effective are background checks on employees (6.4/10 rating) and Reward / Bounty schemes for whistle-blowers (5.6/10 rating). However, among the small number of authorities where a Reward / Bounty scheme for whistle-blowers is used, it is perceived to be the most effective prevention measure (10/10 rating)

Turning to fraud **detection measures**, the most used measures by IQ-Net authorities are on-the-spot check/audits and internal fraud reporting mechanisms, both used by 96 percent of respondents. A second group of measures was used by 70-85 percent of IQ-Net authorities:

- identification of fraud indicators / red flags (84 percent);
- fraud risk-assessment on project applicants/beneficiaries (82.1 percent); and
- data analytics/mining techniques (70.8 percent).

Less than a quarter of IQ-Net authorities (23.5%) used RACER indicators to monitor the efficiency of fraud measures.

Table 5: Fraud detection measures implemented by IQ-Net authorities and their perceived effectiveness

Detection Measures	Usage (%)	Effectiveness Rating (0-10)
On-the-spot checks / audits	96.4	9.0
Internal fraud-reporting mechanisms	96.4	8.4
Fraud risk-assessment on project applicants/beneficiaries	82.1	7.7
Data analytics / data-mining techniques	70.8	7.6
Fraud hotline for whistleblowers	61.5	7.1
Identification of fraud indicators / red flags	84.0	7.0
EU Arachne risk-scoring tool	66.7	5.4
RACER indicators to monitor efficiency of measures	23.5	3.8

Source: EPRC survey of IQ-Net members

The measures with the highest perceived effectiveness ratings are on-the-spot checks/audits and internal fraud-reporting mechanisms, with ratings of 9/10 and 8.4/10 respectively. Half of the measures have an effectiveness score of 7.0 - 7.7 out of 10, namely:

- fraud risk-assessment on project applicants/beneficiaries;
- data analytics / data-mining techniques;
- fraud hotline for whistle-blowers; and
- identification of fraud indicators / red flags.

The measures perceived to be least effective are the EU ARACHNE risk-scoring tool (5.4/10) and RACER indicators to monitor efficiency of fraud measures (3.8/10). While the perceived

effectiveness of RACER indicators increases significantly to 6.3 out of 10 for respondents that use the measure, it still has the second lowest rating of fraud detection measures.

4.2 Proportionality

Formally, proportionate ESIF fraud risk management tailored to the level of risk is ensured through the fraud risk assessment, with anti-fraud measures developed according to the likelihood of fraud, impact and the effectiveness of existing controls. However, there are diverging views about the level of proportionality in practice.

A number of IQ-Net authorities consider fraud risk management to be proportionate, with administrative requirements and efforts perceived largely in line with needs and obligations to prevent and detect irregularities and fraud (DK, Eng, NL, Pom, Vla, W-M). This is facilitated by the availability of new tools for a better targeting of project control samples (DK) or due diligence checks, such as ARACHNE; the introduction of thresholds for fraud assessment based on grant amounts and frequency of assessment (e.g. Wal); or because of the limited size and scale of programmes and beneficiaries (e.g. Biz, Vla). While the approach underpinning the FRA is considered proportionate in the Netherlands, simplification of rules could help to make fraud risk management tasks easier for MAs; for beneficiaries, the burden is already minimal because of short checklists.

For other IQ-Net authorities, it is the initial effort to set up fraud risk management systems that is viewed as demanding with subsequent steps being more straightforward and proportionate (Austria, FI – Helsinki-Uusimaa).

Another group of IQ-Net authorities consider **the administrative burden associated with fraud risk control to have limited proportionality or to be disproportionate to potential fraud risks** for several reasons:

- the increasing complexity of managing fraud risks and the associated requirements;
- a large number of various sources / systems used for collecting and managing fraud risk related information, requiring a significant effort in terms of articulation, cross-checking and validation;
- the stringency in the use of ARACHNE;
- the perception that some of the listed fraud risks are not necessarily relevant;
- vagueness of some red flags, not necessarily indicating actual fraud;
- lack of sampling control methods utilised or/and no additional statistical or analytical methods for risk identification in place.
- evolving requirements and requests for information following the approval of management and control systems.

Lastly, some MAs consider that the **fraud risk management system did not lead to a significant difference in the number of controls and additional burden** due to the fact that there were already a large number of controls required (e.g. SK).

5 MONITORING AND EVALUATING FRAUD RISK

In line with the obligations to undertake fraud risks assessments and put in place effective anti-fraud measures, mechanisms have been developed to monitor and evaluate the effectiveness of fraud risk management measures and systems.

Across most IQ-Net programmes, **the effectiveness of fraud risk management measures and systems is monitored and evaluated based on the regular analysis conducted as part of the Fraud Risk Assessment process** (e.g. AT, DK, EL, ES, FI, HR, PT, W-M), with the scoring often done via the adopted fraud risk self-assessment tool (e.g. AT, EL, HR, NL, Pom, PT, SK, W-M).

This analysis is periodically undertaken **with fraud risk-assessment systems and methodologies regularly being revised and updated** during the programme period. For instance, in Finland, the MA has a process of annual self-assessment of risks and fraud risks, while in Austria, the Netherlands and Vlaanderen, there is two-yearly (or more regular, if necessary) revision of the fraud risk assessments. In Portugal, although no specific calendar is foreseen, fraud risk-assessment methodologies can be reviewed when deemed necessary.

Anti-fraud measures are also monitored in the context of audits carried out by the relevant bodies, with the results incorporated into the associated measures and revisions (e.g. PT, SK, Vla). For instance in Vlaanderen, the system may be adapted in response to the upcoming conclusions of the Audit Authority in the context of its system audit on anti-fraud measures. Similarly in Portugal, the AA/AFCOS carried out an audit (in 2020) on the fulfilment of recommendations and monitoring of the existing anti-fraud measures, althought the results are not available at the time of writing. In Slovakia, monitoring and evaluation are performed within the fraud risk management working groups, drawing on the findings on irregularities from internal and external audits and controls (see Box 7).

Box 7: Monitoring and evaluation of fraud risk measures in Slovakia

In Slovakia, monitoring and evaluation are generally performed within the fraud risk management working groups/parties. The process draws on findings on irregularities from internal and external risk controls/audits/certification verifications. These are summarised in a table format/Excel sheet. Based on these findings, fraud risk is tracked and assessed in terms of whether the correct risks were identified initially, and whether effective measures were taken to address them. As a result, the Working groups/parties can decide to increase the numerical value of the risk level or increase the associated anti-fraud measures.

In the case of the MA for OP HR and OP IROP, this monitoring and evaluation process takes place annually. In other cases (MA for OP QoE and IB-MoE for OP II) FRM is set up as cycle of 5 phases and the monitoring and evaluation process takes place at the 5th phase. The assessment of risks and their levels is analysed based on findings of the internal and external risk controls as well.

Source: IQ-Net fieldwork

The OECD[10] recommends using measurement criteria/indicators based on EC guidance and fraud risk management scorecard tools (see Box 8).

Box 8: OECD proposals on monitoring and evaluation mechanisms for effective fraud risk management

The OECD recommends a systematic approach to fraud risk management including the development of monitoring and evaluation mechanisms, such as scorecards, that capture a wide range of risk management components and activities.

This involves developing targeted tools to structure the evaluation process in order to systematise and integrate monitoring and evaluation activities undertaken by the risk management working groups and risk management functions in MAs.

Targeted tools should be based on key indicators and easily interpreted templates allowing to measure the main aspects of risk management practices and anti-fraud policies, such as scorecards using numerical scoring or a traffic light system to indicate whether the different elements are functioning effectively or require improvements.

Scorecards should cover a wide range of components and measures relating to fraud risk management, with their development requiring an assessment of the MA's anti-fraud measures and objectives relating to OP implementation.

Source: OECD (2019) op. cit.

Monitoring and evaluation of fraud risk measures can also be subsumed within **broader reviews or evaluations of the management and control system**. For instance in Finland, both the MA and the IBs have to assess and update the MCS on an annual basis, and fraud risk management measures are asessed as part of this. The Welsh MA puts most emphasis on their Review Panel for the Anti-Fraud risk register. This is a panel of all interested parties from within the MA (including verifications team, payments team, project management division, and the auditor authority as observers). The panel meets every six months to review all risks including fraud.

Specific monitoring arrangements also exist with regards to conflict of interest. For example in England, there are distinct processes for monitoring potential conflicts of interest in relation to programme monitoring committee decisions or procurement (Box 9).

Box 9: Monitoring procedures for conflicts of interest in England

In England, monitoring of conflict of interest relating to PMC decisions takes place at least once in every 12-month period, and on other occasions at the discretion of the PMC Chair, all members must review the information relating to him or her contained in the register of interests and declare that the information is correct or make a further declaration if necessary. Members must also report any suspicions of fraud or malpractice to the Chair, who will refer the matter to the relevant MA or public authority.

In relation to procurement, grant recipients must put in place procedures for storing and monitoring declarations, such as a special register (with a template being provided in an Annex of the MA's Conflicts of Interests guidance)[11] or management information system for each procurement exercise. A member of staff who is not involved in the procurement exercise should be designated to monitor the declarations and ensure up to date records are maintained. Grant recipients must also conduct additional checks where they received any information about a potential conflict of interest from outsiders with no connection to the procurement exercise.

Source: Terms of reference for the Growth Programme Board (Programme Monitoring Committee), December 2019. https://bit.ly/3lhaaKe

6 BUILDING CAPACITY FOR FRAUD RISK MANAGEMENT

Fraud risk management requires capacity-building through technical assistance, the systematic use of dedicated tools and cooperation with other competent bodies (e.g. investigation, prosecution and judicial bodies). Member States can invest EU funds in administrative capacity to tackle fraud through TO11 – Strengthening institutional capacity and efficient public administration, or through the Technical Assistance priority axis of OPs e.g. by funding staff costs on audit activity or through investments in anti-fraud systems and tools.

The European Commission and OLAF also provide support for activities aiming to build capacity and awareness of the authorities involved in ESIF management, e.g. via training, workshops, guidance, facilitating "peer-to-peer" cooperation and exchange and other measures. The Commission DGs responsible for ESIF (DG REGIO, DG EMPL and DG MARE) have recently revised their multi-annual Joint Anti-Fraud Strategy identifying concrete actions to further improve fraud prevention and assistance, including by providing a tool-box for training with an e-learning platform, raising awareness and other supporting initiatives.

6.1 Capacity for fraud risk management

The allocation of resources for carrying out control of fraud risks is generally deemed sufficient by most IQ-Net programme managers (e.g. AT, CZ, DK, EL, NL, Pom, Sco, Vla, Wal, W-M). This is due, among other things, to factors such as limited instances of fraud (e.g. Sco), clear definition of responsibilities (e.g. EL), with designation of dedicated staff members and contact points for dealing with fraud risk specifically (e.g. AT), significant level of experience in fraud risk controls (e.g. EL), as well as the effectiveness of training for staff (e.g. AT, CZ IROP, Eng, HR, Sco, W-M) and fraud risk- awareness measures for the authorities involved in ESIF implementation (e.g. AT, HR, W-M). Additional resources dedicated to counter fraud activities have not been deemed necessary (e.g. Biz, FI, SK, Vla, Wal) despite the increasing administrative and time demands (e.g. Biz).

Where the resourcing of fraud risk management is not considered sufficient, the following explanatory factors have been highlighted:

- lack of human resources available within MAs/IBs and other national authorities (e.g. audit) to effectively manage fraud risk (FR), particularly given the extensiveness of the required checks and controls (SK);
- lack of reinforcement in human resource capacity in line with the expansion of fraud risk management- related responsibilities (SK);
- competing tasks/deadlines for staff and time constraints (SK, Pom[12]); and
- lack of knowledge of fraudulent irregularities (FR) and insufficient training in fraud risk management (SK).

6.2 Capacity-building activities

Across IQ-Net programmes, **training and awareness-raising events are common**. In many cases, training is a central element of capacity-building, and efforts are pursued to train staff of all or most bodies involved in ESIF management, with a particular focus on the MA and in some cases IB staff.

Most MAs provide formal trainings to staff on fraud-related issues, which take various forms, e.g. training courses, workshops, e-learning modules etc. For example, in Croatia training is organised for employees of MAs and all MCS bodies; similarly, all MA staff in the UK programmes undergo relevant training (Eng, Sco, Wal). In France, between 2016 and 2019, around ten training actions have been organised specifically with MAs. In Spain, the central MA at the Ministry Finance (DG EU funds) offers seminars and courses throughout the year to keep staff updated on developments and best practice.

Training activities are organised not only by the MAs, but often also by other entities, including national ESIF coordinating authorities (e.g. CZ) and other coordinating bodies (e.g. the Central

Contact Point for cooperation with OLAF – CZ, the National office for OLAF – SK), AAs (e.g. CZ), IBs (e.g. AT,[13] SK[14]), specialised training bodies (e.g. Federal Administration Academy – AT) and others.

Along with **voluntary training** activities (e.g. a voluntary e-learning module developed by the Antimonopoly Office of the Slovak Republic in cooperation with the National office for OLAF), there are also elements of **mandatory training** across some IQ-Net programmes. For example in England, MA staff must take mandatory civil service annual counter fraud online training, while a compulsory annual update to the fraud risk training for all MA staff takes place in Scotland. In Czechia, each employee of the Ministry of Regional Development has to take an e-learning course including also this topic at least once every two years, and in Croatia, there is an obligatory education course on irregularities. In addition, public servants in Croatia are encouraged to take public procurement exam and obliged to continue additional training on the topic, to renew the validity of their accreditation every three years.

The thematic focus of training can cover all aspects of anti-fraud policy, individual tasks and responsibilities and reporting mechanisms (e.g. W-M). Where more specific knowledge is needed, **specific courses** for anti-fraud qualifications are used. Some examples include:

- staff training on **ARACHNE** (e.g. CZ, NL, SK) and company information, for strengthening the capacity of navigating in the ARACHNE database and verifying applicant/grant recipients data;
- training focused on identifying signs of fraud (**red flags and risk indicators**) more generally and responding to such actions (e.g. SK, W-M);
- training sessions focused on **sample controls**, aiming to facilitate the identification of administrative mistakes and fraud cases (e.g. DK);
- seminars on the **protection of EU financial interests** (e.g. CZ, SK);
- training and advice on **reporting irregularities to OLAF** (e.g. CZ);
- **specific training and seminars on related topics**, e.g. irregularities and financial corrections (SK); detection of fraudulent conduct in EU funded projects (SK); corruption prevention – compliance – integrity; integrity and values management in the public service; and internal control systems and risk management (AT).

An important focus of many such actions across IQ-Net programmes is on training employees to distinguish actual fraud cases from administrative mistakes ('normal' errors or irregularities by beneficiaries) (CZ IROP, DK, SK).

Some of the training actions for MAs/IBs across IQ-Net programmes involve the participation of external experts and speakers, e.g. representing investigatory bodies (e.g. FI, PT), audit or certifying authorities (e.g. FI, PT), academic experts (e.g. SK) or consultancies (e.g. CZ). For instance, in Finland training sessions for IBs and the MA involve external speakers from different organisations, including the National Bureau of Investigation, Audit experts as well as

representatives of the CA. In Slovakia, some tailored risk management training for IBs has been provided by academic experts (e.g. from the University of Žilina). In Czechia, a specialised training was organised for employees by Deloitte anti-fraud experts.

Less formal, routine, information exchange activities are also seen as important for building fraud-management capacity. For instance in Pomorskie, on the job training and experience gaining are the main capacity-building activities, while in Vlaanderen, in the absence of formal training initiatives at the Member State or regional level, the MA itself organises informal knowledge exchange and anti-fraud training.

Fraud risk training and capacity-building initiatives also target ESIF beneficiaries and applicants. For example under Czech IROP, seminars are considered crucial for raising risk-fraud awareness of beneficiaries, particularly less experienced ones, and in Wales, training is also provided to applicants. Workshops for users, informing them on the measures taken to prevent, detect and deal with fraud (especially public procurement issues) and the associated consequences are an important part of capacity-building activities in Croatia.

A number of training and capacity building constraints and ideas for improvement have been highlighted:

- the **limited scope** of existing capacity-building activities, both in terms of the number of organised trainings and the number of experts in the field that could be engaged (SK – National office for OLAF);
- a **lack of focus** of trainings on specific aspects of fraud risk management, notably identification, analysis, assessment and monitoring of fraud risks (SK – OP QoE);
- **need for more practical training**, e.g. organised by the EC or law enforcement agencies (CZ IROP); and
- challenges posed by the **Covid-19** pandemic, including interruption of the ongoing training courses or scheduled training actions (CZ MF; SK IROP; PT).

Aside from training actions, **other capacity-building activities** undertaken include:

- **Dissemination of guidance, manuals / handbooks**. For instance, an internal control and risk management manual serves as the overarching tool within the Regional Council of Helsinki-Uusimaa (FI). In the Netherlands, control and accountability procedures are explained in the programme handbooks. Relevant guidance is also available online in a large number of cases.
- **Organisation of meetings and events for knowledge exchange** between MAs and other relevant bodies (e.g. paying units, audit and certification authorities, etc.), including via coordination group meetings (e.g. West Finland; DK) and programme management meetings (NL, W-M, etc.), dedicated networks for exchange of experience (EL), and informal consultations (e.g. Vla).

- **Regular monitoring of relevant guidance, publications and internal information systems**, e.g. monitoring of the OLAF website, ECA reports, domestic public procurement databases and other relevant websites and search engines.

6.3 Use of ARACHNE

To support managing authorities in their fraud risk management controls and checks, the European Commission developed ARACHNE as an integrated IT tool for data mining and data enrichment. A PWC (2018) study[15] commissioned by DG REGIO found that the majority of MAs did not use ARACHNE, although most of the MAs using the tool saw an added value in terms of assessing potential conflicts of interest and identifying red flags. The main challenges regarding the use of ARACHNE related to: data collection and accuracy issues (the incompleteness of the database and outdated data); the high number of false positives for potential conflicts of interest; and legislative barriers, particularly compliance with national data protection laws. Other problematic issues included the potential for creating additional administrative burden, insufficient interoperability of ARACHNE with other national IT tools and databases in use, as well as the need for additional awareness-raising and training on the use and benefits of ARACHNE.

Around half of the IQ-Net Authorities use ARACHNE (CZ, FR, HR, NL, PT, SK, Vla, Wal), in most cases along with other information systems and tools – e.g. domestic registers (e.g. FR) or other databases which are used more widely and/or more regularly, including commercial tools. For instance in the Netherlands (see Box 10) and Slovakia, it is used as a complimentary tool to the Company Register; in Croatia, ARACHNE is used for the purpose of verification, upon regularly monitoring various search engines. In Slovakia, ARACHNE is used along other complimentary tools including Company register, Trade register, NGO register, Criminal Register of the General Prosecutors Office of the SR, Public registers of debtors, FOAF[16] and FINSTAT[17]. The use of ARACHNE as the only tool for fraud detection and prevention is limited (e.g. Vla).

Box 10: Use of ARACHNE in the Netherlands: application and drawbacks

In the Netherlands, ARACHNE is not considered to fully address needs and there is room for improvement in its possibilities. By contrast, the domestic Company Information Register is regarded to be a more reliable, fast and comprehensive database. Currently, the MAs use ARACHNE selectively with the aim to i) discover related parties (making use of the surrounding view, allowing to see the 'tree structure' of Ltd private companies); ii) check for companies in financial difficulty, especially liquidations and requesting SME status; and iii) check for matching, whereby beneficiaries may have received other domestic or EU subsidies for a similar project.

ARACHNE and the Van Dijk database frequently ask to check data entries in their systems, but this goes beyond the scope of the MAs. The evaluation of the ARACHNE pilot (2018-2019), as published by the West MA, concluded the following:

> *ARACHNE could be a good system with added value, but the EC has designed the product in such a way that it falls short in relevant areas for us. This is because ARACHNE is particularly focused on making risks transparent at project level, whereas our control points are more*

partner-oriented. ARACHNE feels like a semi-finished product that still needs to be perfected by the EC.

A few small adjustments would already make for great results. ARACHNE makes a comparison between, for example, infrastructural projects, such as the construction of (rail) roads. The comparison between the costs per constructed km is useful in itself and could provide interesting insights, but in the Netherlands, no infrastructural projects are carried out.

Instead, projects aim at innovation, which is not comparable. Occasionally, ARACHNE brings up a 'related party' that was not yet in the picture.

The question is whether the costs outweigh the benefits. The information from Company Info is often more complete and clear. On the other hand, the EC would like us to use this system in conjunction with FRA and therefore we would not need to set up another system. By our use of ARACHNE, as explained in this memo, our projects are visible to other Member States. We use a mix of systems for the risk analysis of projects, and in line with the anti-fraud efforts of the EC, it is sensible to keep it that way.

Source: Kansen voor West (2020)

Where ARACHNE is not used (e.g. AT, DK, EL, Eng, FI, Pom, Sco, W-M), national/regional IT systems / information sources (e.g. domestic databases – DK, Eng, FI; own checklist – Biz) or other tools / external databases (e.g. AT – CRIF[18]) are in place, offering similar functions. **Future adoption of ARACHNE is** however **not ruled out** in some cases (e.g. EL, FI). In England, the MA had planned to implement ARACHNE and started to enter data into the system in March 2020, however it had not been rolled out prior to UK lockdown due to Covid-19 and it now seems unlikely.

The **views on the benefits of ARACHNE for specific risk management purposes are not consistent** across IQ-Net programmes. For instance while in Croatia it is seen as a particularly useful tool for the purpose of *verification*, in Slovakia (IB-MoE for OP II) its usefulness is mainly perceived it terms of *detecting possible fraud* by identifying risk indicators rather than verification of fraud, where other tools come into play. Similarly, in Vlaanderen it is found especially useful for preventive research and gathering information, e.g. detection of ties between beneficiaries and companies. **Other perceived benefits of ARACHNE relate to**:

- its application in public procurement, via providing information concerning involved entities and the relationships among them (SK);
- the search function for news media (DK);
- the ability to focus the activities and human resources on riskier users, projects and contracts, thus helping improve the efficiency and effectiveness of management checks.

Main **criticisms regarding the application of ARACNHE** relate to the following.

- **Data limitations**, including **lacking and outdated data**. Several IQ-Net managers have raised the issue of a significant lack of data, calling into question its liability. It has, for instance, been noted to contain only data that the subject is willing to communicate about itself and which are publicly available (CZ), not include Horizon beneficiaries (NL), or lack appropriate data for a large number of criteria in use (CZ). Moreover, lack of up-to-date data has been noted, e.g. repository of data only from the 2014-20 period (CZ) or absence of updated data (3 years old) on companies (EL).

- Existence of **other tools used domestically**, and **lack of interoperability or information exchange with other databases and systems** (CZ, FI, FR, HR, NL, PT, SK). A large number of different information sources and registries are consulted for fraud risk management purposes, however, integrated solutions or a centralised database are absent. Among other things, this has been noted to hinder the provision of appropriate data or its interpretation (CZ) and require a substantial additional effort from staff consulting and analysing the different data sources, in terms of articulating information and verifying it across different databases (PT).

- **Limited scope for application**. For instance in Vlaanderen, ARACHNE is mainly suitable when the beneficiaries are companies (i.e. a minority in ERDF Vlaanderen), whereas the majority of beneficiaries are public bodies. Little scope to adapt the type of project has also been noted, making peer groups largely unsuitable.

- **Identification of a large number of 'false' red flags**, and limited explanatory power of risk analysis**.** The large number of false positives, combined with little differentiation between high and low risk cases and impossibility to 'remove' a red flag have been noted to create a significant and non-proportionate managerial burden by obliging the MA to check the flagged risks (e.g. EL, Vla). In many cases, high risk scores shown in ARACHNE are in practice not associated with actual fraud risks, can be explained (e.g. the activities indicator), or do not provide any meaningful information (e.g. bankruptcy in public entities). On the other hand, the Welsh MA has noted the lack of ARACHNE's ability to identify conflicts of interest readily.

- **Varied usage across MAs**. The application of ARACHNE and its benefits vary across MAs (e.g. FR, PT, SK, Vla), which, among other things, may relate to the different degree of relevance of the data stored for the specific types of projects funded under different OPs (e.g. SK). A more universal use of ARACHNE across OPs is seen as potentially beneficial in some cases (e.g. Vla).

- **Complexity**. The software is considered complex, not very intuitive and demanding in human resources by a number of IQ-Net managers (e.g. FR, EL), and its effective use requires specialised training (e.g. CZ, SK), which is not always in place.

- **Legal constraints**. This includes incompatibility with national legislation for data protection (e.g. DK[19]) or legal restrictions in incorporating ARACHNE in contracting procedures, if it could be used by beneficiaries acting as contracting authorities (EL).

In this context, the main **suggestions for improvement** relate to the following:

- need to increase the interoperability, integrated solutions and information exchange with other database systems (e.g. CZ, FI, FR, HR, NL, PT, SK);

- need to enhance training, exchange of knowledge and sharing of good practices on how to efficiently use ARACNHE, including through practical training, specialised workshops, production of handbooks of good practices etc. (e.g. CZ, SK).

6.4 EU capacity-building assistance

There is varied perception of the usefulness of the capacity-building assistance provided by the European Commission, and varied degree of use of its various modalities across IQ-Net programmes.

While all capacity-building measures offered by the Commission are considered useful in some cases (e.g. PT, SK, Vla, W-M), their use is more limited or less systematic in others (e.g. DK, FI, NL, SK), not least due to the insufficient level of awareness of the existing opportunities among the MAs / IBs (e.g. SK) or the relatively lower level of concern with fraud-related challenges more generally (e.g. DK).

The usage and perceived utility of specific capacity-building measures offered by the Commission vary across programmes.

6.4.1 E-learning module

The e-learning module is perceived to be useful e.g. by the Finnish MA, including as it gives possibilities to reach out more staff members within the IBs. While not yet offered by the EC to be used under the Czech IROP, it is perceived as potentially desirable. According to the Dutch MA, the potential of the e-learning module could be improved by focusing it more on building capacity in the area of digital fraud, including by providing concrete practical examples.

6.4.2 Guidance

Commission guidance for anti-fraud measures is generally viewed to be useful (e.g. DK, NRW, Pom, PT, SK, W-M), including in terms of providing the basis for domestic guidance documents and tools. At the same time, the need for greater methodological leadership by the Commission has also been mentioned (CZ IROP), as well as the need to better adjust the application of guidance to the specific national contexts (e.g. FI) and generally make it more targeted as opposed to generic (e.g. Wal).

6.4.3 Online toolbox of case studies / good practice

Toolboxes of case studies and good practices are found to be useful (e.g. FI, NL, Pom, PT, SK, Vla, W-M) for providing practical examples and awareness-creation. A constant need for continuation and expansion of further cooperation through exchange of good practice between member countries has also been stressed (HR).

At the same time, the **following changes are viewed desirable** by some programme managers:

- greater focus on digital fraud prevention (NL);
- more emphasis on case studies representing concrete situations, e.g. with descriptions of concrete financial amendments, cases of concrete court dispute and decisions taken from the different MSs (CZ IROP);
- greater number of case studies / good practice examples more relevant to the specific national contexts (e.g. FI).

Apart from the online toolbox made available by the EC, other channels for sharing and learning of best practices across Europe and beyond are used by IQ-Net programme authorities, including conferences and seminars (e.g. Wal), an OECD toolbox (e.g. EL), or participation in the OECD missions (e.g. SK). For instance several of the MAs took part in the OECD mission in Slovakia, where they were presented with best practices from different European countries, which is viewed as a useful experience. The staff of the Danish MA have recently contributed with their own experience on developing and using the OBS lists to PWC Luxemburg for the collection of good practice cases.

6.4.4 Training provision

A number of IQ-Net programme authorities use the training provided by the Commission, including on the use of ARACHNE (e.g. SK, Wal), and consider it useful (e.g. FI, HR, PT, SK). Some programme managers view the online training as particularly practical as this allows a wider participation (FI). While not yet used under the CZ IROP, the Commission training offer is viewed as desirable. A relatively low incidence of fraud-related issues may account for lower participation in fraud specific trainings in some cases (e.g. FI – Regional Council of Tampere region), while the different contexts of the Member States participating in training may make it difficult to go into detailed discussions, often making them rather generic (FI).

6.4.5 'Integrity pacts' and 'peer-to-peer' cooperation and exchange

Several IQ-Net countries have participated in integrity pacts (e.g. EL, HU, PL, PT, SK).[20] The MA of CZ IROP was offered an integrity pact, although it was not perceived to be useful and was not used. Participation in 'peer-to-peer' cooperation was also considered by some programme managers (e.g. EL, Eng), but has not come to fruition as yet, including due to the Covid-19 outbreak (e.g. EL).

7 LESSONS AND PLANS FOR 2021-27

7.1 The added value of fraud risk management

The increased focus on fraud risk management in 2014-20 has led to systematic changes in fraud risk management strategies, procedures and measures across EU countries and regions. At the same time, in many cases this is seen essentially as a path-dependent evolution and **improvement of the previously existing practices** rather than a radical shift in direction (e.g. AT, FR, PT).

The main positive effects arising from the reinforced emphasis on fraud risk management in 2014-20 include the following.

1. **Raising awareness.** Across IQ-Net countries and regions, the increased focus on fraud risk management is seen to have promoted greater awareness of the issue, by giving it more visibility and focus, generating more discussion, and contributing to the development or strengthening of a fraud risk culture (CZ, CZ IROP, DE, EL, Eng, FI, FR, NL, PT, SK, Vla). The additional awareness created by such increased focus (including due to the obligation to undertake the fraud risk assessment) has led to a change of mind-set and more proactive role of the MA in fraud prevention and management (Vla) with reinforced appreciation of the importance of implementation going beyond formal compliance with regulatory requirements (SK).

2. **Building new domestic skills in fraud risk management.** The reinforced fraud risk agenda has helped to increase staff capacities and develop their skills in fraud risk prevention and detection with benefits for both the current and future period (Biz, FI, FR, HR, SK, W-M).

3. **Promoting a more integrated, structured and targeted approach to fraud risk management.** The increased focus on fraud risk management has promoted a more structured and targeted approach to managing fraud risk (Eng, Pom), a more integrated approach across all levels of fund management and audit (FR) and more robust measures (DE, EL).

4. **Increasing transparency.** According to the ÖROK (AT), the whole fraud-risk management system has become more transparent.

5. **Increasing the effectiveness of fraud risk management and reducing the risk of fraud.** New or improved fraud risk management procedures in 2014-20 have resulted in improved detection of potential fraud risks and identification of fraudulent practices at an earlier stage, as well as and the creation of adequate responses to these practices and risks (DK, HR, SK). This has overall allowed to increase the effectiveness of fraud risk management and reduce the risk of fraud. For instance in Denmark, the OBS lists that are based on data analysis capture potential fraud cases to a higher extent than previously, e.g. the cross-referencing of CVR/company numbers between beneficiaries and suppliers entails that this type of potential fraud cases are detected by the IT system – which would previously only be discovered in connection with sample controls.

Increased administrative burden is the main negative effect of the increased focus on fraud risk management (e.g. Biz, CZ, CZ IROP, EL, some regions in FI, FR, HR, SK, Pom, Vla, W-M). In many cases, managing authorities have been allocated further responsibilities in fraud risk management without increased resources/staff. Administrative burden is created by technical aspects of data exchange, e.g. the integration of the ARACHNE software (e.g. FR, Vla), as well as organisational aspects of designing and revising control procedures and internalising new requirements, such as the fraud risk assessment tool (e.g. EL, some regions in FI, Vla). In addition, according to the Warmińsko-Mazurskie MA, management and control systems, including in the area of risk management, are generally becoming increasingly complicated and introducing additional obligations that do not directly flow from the legal regulations.

7.2 Lessons for 2021-2027

Fraud risk management procedures and measures in 2014-20 have evolved significantly reflecting the growing attention to the topic at EU level, the increasing scope of regulatory requirements and the creation of new tools (e.g. ARACHNE).

Partly as a consequence of these changes, **the importance of continuity and stability** has been emphasised, in the sense of avoiding any major changes to the current system, which is seen as working well (e.g. AT). Ensuring coherence is also seen as important due to the fact that the current and the future systems will have to work in parallel for some time. In other cases, while a continuation of the current approach is generally supported, the need for better access to effective tools for fraud risk management has been stressed (e.g. Pom).

Overall, the **main lessons drawn from 2014-20 for the future 2021-27 period for improving effectiveness and proportionality** in fraud risk management relate to cooperation, harmonisation and interoperability; simplification; flexibility and proportionality; capacity building; and early detection and prevention.

7.2.1 Cooperation, harmonisation and interoperability

The **main lessons learnt** for most IQ-Net programme authorities are the need for greater: (i) connectivity and harmonisation between the different databases and information systems; (ii) institutional coordination and cooperation; and (iii) experience and information sharing is.

- There is scope for improving the **connections and information exchange between the different data systems** (e.g. CZ, FI, FR, HR, NL, PT, SK). Among other things, this implies a greater interoperability between different databases, greater centralisation of relevant information and wider possibilities for sharing it. As mentioned above (see Section 3.2), a large number of different information sources and registries are consulted for fraud risk management purposes, but integrated solutions are largely absent. From the Portuguese point of view, it would be of an added value to create the conditions so

that MSs can develop their tools with legal support that allows access to personal data[21] and that imposes interoperability between various information systems, imposing the need to create a unique repository of management information from the Member States[22] and the possibility of sharing it among the various national bodies and with the systems of the other Member States and bodies involved in combating fraud.

The **integration of the ARACHNE software** is seen an important element of this (e.g. FR, SK, Vla). Integrated solutions and a shared interface amongst managing authorities could improve the knowledge, enable an exchange of best practices and experiences in fraud risk management, facilitate the feedback of information to OLAF, and decrease the risk of error.

- **There is scope for improving institutional coordination and cooperation** on fraud-related matters (e.g. Biz, SK, W-M). In 2021-27, cooperation and the exchange of experience and information between institutions involved in ESIF implementation, state authorities and EU institutions aimed at preventing, detecting and prosecuting fraud should be further developed. For instance in Bizkaia, more coordination among different bodies and levels is needed in audit activity. In Slovakia, a stronger involvement and leadership of the Central Coordination Body in the potential establishment of an exchange platform reflects the need for better coordination and exchange between MAs and other related bodies.

- **Exchange of experiences should be improved**. Generally, the sharing of good practice and experiences among all relevant actors should be intensified (e.g. CZ, W-M).

7.2.2 *Simplification*

There is need in increasing simplification and decreasing the administrative burden (e.g. DK, FR, HR, SK), e.g. by simplifying the legislative framework or at least not adding new requirements (e.g. EL), lowering the reporting threshold for irregularities (e.g. FR), developing the practice of the single audit by the EC and a proportionate approach to controls (e.g. FR) – supported by a simpler management architecture (e.g. FR). It has been highlighted that heavy and complex procedures lead to low uptake (e.g. by the IBs) and high number of errors (HR), hence the introduction of more simplification measures is pertinent.

Enhanced use of SCOs might be able to facilitate data analysis and lead to fewer potential fraud cases. This is perceived to be particularly relevant in the programmes where most cases involve mistakes in the reporting rather than fraud (DK). By contrast, others note that the wider use of SCOs focused on achieving specific objectives as opposed to spending and controlling financial compliance, can imply a heightened risk of fraud. While there is as yet no comprehensive evidence to support either view, the issue is on the agenda at EU level and monitored by OLAF.

7.2.3 *Flexibility and proportionality*

While there is demand for specific uniform tools (e.g. integrated IT solutions) and common guidance from the EC, Member States also request flexibility to adapt any new requirements to their domestic operating environment and legal context (e.g.

EL, FI, PT). Proportionality is an regarded as critical from an implementation perspective (e.g. EL, Vla) and should be taken into account when new tools are introduced. According to Greek authorities, the use of Commission tools should be optional and Member States should be allowed flexibility to adopt their own systems. Similarly, ÖROK (AT) have concerns that ARACHNE might become compulsory, which is something they would not favour. In Vlaanderen, the assessment of the functioning of the current management system by the AA will be crucial to maintain proportionality of anti-fraud management.

7.2.4 Capacity-building

There is need to further enhance the anti-fraud capacity of the authorities involved in ESIF management, including by improving the following aspects.

- **Human resources dedicated to anti-fraud tasks**. The enlargement of the human resources of the anti-fraud coordination service and MAs in charge of ESIF applications appraisal is seen important to enable an adequate detection, control and response to irregularities and a promotion of a coordinated anti-fraud approach in France.

- **Training / skills enhancement**. The necessity to increase domestic skills (e.g. SK) and further develop educational activities (W-M) has been stressed. The Welsh MA emphasised the particular value of the specific training that was carried out for the payments and verifications teams within the MA, based on actual cases. This training raised awareness and was particularly impactful as the documents used had actually been used to perpetrate fraud, emphasising the need for MA staff to challenge things that did not look right.

- **Provision of information and guidance** (e.g. CZ, EL, FR, Wal), including through sharing **examples of good practice** (e.g. CZ IROP, EL, HR, W-M). Among other things, there is need to improve the quality of available information regarding fraud with European funds (e.g. improving the content of the EC's annual report on protection of financial interests of the EU and fight against fraud with data supplied by police and judicial authorities of each Member State) (FR) and ensure greater methodological leadership from the EC (CZ). More specifically, clarification on how EC auditors will test the MAs' control systems, including ARACHNE, would be welcomed (Wal).

  Publishing examples of good practice from individual Member States in the fight against fraud could also help improve anti-fraud action at EU and domestic level (HR), and sharing of good practices should be intensified (CZ IROP). The role of the Commission in this regard should be further developed, e.g. in terms of elaborating of a compendium or toolbox of good practices, which could assist practitioners with fraud risk management and improve its effectiveness and proportionality (CZ, W-M).

7.2.5 Early detection and prevention

Focusing on preventative measures and embedding counter fraud management at an early stage in management and project appraisals processes, including by strengthening the early warning system for irregularities,[23] would help to save time and effort and increase the effectiveness of fraud management (e.g. Eng, W-M). In addition, consideration should be given to extending additional control mechanisms to

areas and sectors of the market in which an increased risk of fraud has been identified in 2014-20 (W-M). Overall, the management systems should be designed more with fraud in mind to enable information to be gathered and shared more easily (Wal).

In this context, the value of sound fraud risk assessments has been emphasised (e.g. HR, NL), optimising the existing processes (SK). As noted, the FRA is seen as important to promote awareness and discussion (NL), helping to understand fraud risk knowledge gaps and tailoring responses to needs accordingly (HR).

Finally, recent studies by the Court of Auditors and OECD provide lessons and recommendations for current and future programmes. The ECA 2019 Special Report Combating Fraud in Cohesion Spending assessed whether MAs have fulfilled their responsibilities at each stage of the anti-fraud management process. While the court found improvements in fraud risk assessments and the design of preventive measures, it considered that more proactive fraud detection, reporting and coordination was needed. The ECA recommendations were to:

- develop formal strategies and policies to combat fraud against EU funds;
- make fraud risk assessment more robust by involving relevant external actors in the process;
- improve fraud detection measures by generalising the use of data analytics tools and promoting the use of other 'proactive' fraud detection methods;
- monitor fraud response mechanisms to ensure they are consistently applied; and
- support the expansion of the Anti-Fraud Coordination Services' (AFCOS) function to improve coordination

A complementary ECA Special Report 'Fighting fraud in EU Spending' identifies four key recommendations for tackling fraud in all areas of EU spending including specific references to Cohesion Policy:

- put in place a robust fraud reporting system, providing information on the scale, nature and root causes of fraud;
- achieve better coordination, ensure that strategic fraud risk management and fraud prevention would be clearly referred to in the portfolio of one Commissioner; and adopt a new comprehensive anti-fraud strategy based on a comprehensive analysis of fraud risks;
- intensify fraud prevention activities particularly by calling on the Member States to identify and flag fraudulent economic operators and the private individuals linked to them, and urging Member States to make active use of the ARACHNE database to prevent fraudulent and irregular use of EU funds; and
- give OLAF a strategic and oversight role in EU anti-fraud action.

According to an OECD study on Fraud and Corruption in ESIF, key areas for improving risk management are:

- strengthening the effectiveness, coherence and co-ordination of existing strategies for managing fraud and corruption risks and implementing risk-based control activities in EU-funded projects;
- improving the effectiveness of methodologies and tools for identifying and assessing fraud and corruption risks in OPs, including the use of data for analytics, leveraging risk assessments to inform decision making, and monitoring and evaluation of fraud and corruption risk management; and
- enhancing activities and mechanisms that promote a government-wide culture of risk management related to ESI Funds, such as working groups, awareness-raising initiatives and technical training.

The OECD sets out five key tips to protect EU Funds from fraud and corruption:

a) develop cooperation mechanisms at national level for detecting and tackling fraud;

b) maintain risk registers and integrate risk-based control activities;

c) use data-driven analysis to inform detection and action;

d) improve risk governance by establishing counter-fraud policies; and

e) regularly monitor and evaluate to improve your fraud risk management approach

A more detailed set of fraud risk management recommendations tailored to the project cycle is set out in Box 11.

Box 11: Fraud risk management actions during the policy cycle

Project application and selection

- Ensuring an adequate degree of transparency around the selection process by publishing and recording all calls for applications;
- Ensuring conflict of interest provisions are in place and applied to Evaluation Committee members;
- Requiring staff and members of the Evaluation Committee to disclose their family members' private interests where potential conflicts of interest may arise;
- Cross-checking information and making use of relevant data analytics techniques to make sure that submitted information is correct;
- Making sure that members of the Evaluation Committee sign a declaration to show their commitment to following relevant codes of conduct and integrity standards;
- Putting in place a mechanism within the internal audit function for a secondary review of individual decisions or a sample of decisions made by the Evaluation Committee.
- Making sure that staff are aware of available channels to report suspected fraud, corruption or integrity breaches during the project selection process.

Project implementation

- Ensuring that a comprehensive audit trail is maintained to enhance On-the-Spot (OTS) checks and management verifications once the project is well under way, as well as during the project closure and evaluation stage;

- Providing standards of conduct for third parties such as contractors, subcontractors and experts, primarily by implementing a specific code of conduct that includes clear examples of activities that will compromise integrity standards, as well as outlining applicable sanctions for integrity breaches;
- Ensuring all actors have similar access to tender information;
- Establishing a sound and comprehensive e-procurement system for the complete dissemination of public procurement information;
- Ensuring that tender designs are complete and accurate, and that a technical commission undertakes site surveys;
- Where possible, carrying out a parallel independent procurement evaluation to strengthen detection of collusion, bid-rigging and favouring a particular contractor;
- Requiring bidders to comply with certain standards to participate in the bidding process for projects considered at-risk to fraud or corruption, and those with high investment value;
- In the tendering phase of procurement processes, using a two-envelope approach whereby the envelope containing the price is only considered following a technical evaluation; and
- Ensuring that profit and labour costs are separated from the rates for materials and equipment.

Project closure and evaluation stage

- Ensuring that auditors are subject to specific codes of conduct regarding beneficiaries, contractors and other third parties;
- Putting in place certain conflict of interest provisions for evaluators and experts, i.e. require such individuals to sign an absence of conflict of interest declaration;
- Cross-checking information across available databases to ensure that submitted information is accurate;
- Ensuring that Supreme Audit Institutions (SAI) have the authority and capacity to provide external oversight of the management of European Structural and Investment (ESI) Funds.

Source: OECD (2019)

7.3 Planned changes in 2021-27

For a range of IQ-Net Programme authorities, **changes to fraud risk management in 2021-27 are still to be determined** (e.g. CZ, PT, Pom, W-M), as the management and control models for the next period are not yet completely defined, partly because EU and domestic legal frameworks are still to be finalised.

That said, **no major changes are foreseen** in a number of cases where the current approach is expected to continue in the future (e.g. AT, Biz, DK, NL, Sco, Vla), not least because the current frameworks are considered to be working well (e.g. DK, NL, Sco).

Where changes are expected, they relate to the following aspects.

- **Use of ARACHNE**. The future approach to ARACNHE and any adjustments are currently being considered, with any modifications still to be decided (e.g. NL, SK, Wal, W-M). In the Netherlands, the added value of ARACHNE will be discussed between anti-fraud actors, while in Warmińsko-Mazurskie, there is increasing consideration of introducing the obligation to use this tool in risk analysis. The Welsh MA are awaiting information as

to whether they will retain access to ARACHNE, and in Slovakia, adjustment to the ARACHNE system is foreseen in accordance with users' recommendations.

- **Governance changes**, including **increased institutional coordination**. In France, the potential suppression of the certification authority could leave the MAs with further responsibility of integrating an additional accounting function, with the certification mission having to be carried out by an internal control service. In Slovakia and Warmińsko-Mazurskie, cooperation and information exchange between relevant institutions could be expected. For instance, the Slovak Central Coordination Body is expected to play a more active role in the communication and exchange among relevant authorities and bodies and in the organisation of training activities.

- Other anticipated or proposed changes include greater focus on **conflicts of interest** (FI), establishment of new procedures and practices in line with the new EU directive on the **protection of whistle-blowers** (FI); and increased focus on timely **anti-fraud education and workshops** and the **application of good practices** from previous periods in order to more effectively and thoroughly combat fraud (HR).

Finally, **a number of IQ-Net authorities are reviewing the possibilities of risk-based management verifications**, as foreseen in Article 68 (2) of the draft CPR for 2021-27,[24] particularly with regard to project sampling. For instance, the Czech IROP MA welcomes the proposed changes as it would allow the most risky projects to be selected (e.g. for assessment of request for payments etc.). This change could bring significant simplification, but this will also depend on how the EU rules would be transposed into national legislation/guidance. In Slovakia, risk based management verifications are not currently carried out although regulatory and conceptual steps have been made to employ them as of 2021. All implemented projects are subject to on-the-spot checks. Sampling is not allowed in the verification of payment claims. There is currently no particular plan as to how such new method of risk-based management verification could/will be implemented. Lastly, a number of IQ-Net programme authorities **envisage carrying out risk-based management verifications relying on the experience accumulated in the 2014-20 period** (e.g. EL, HR, NL, Pom, Vla, W-M).

For instance, in the Netherlands verifications are done using both desk checks (on project progress reports) and on-the-spot checks (through the risk analysis checklist, an observation tool, and a risk profile). The West MA has a randomised observation tool (40 percent of project declarations) and also does a select check on suppliers listed on the invoices at risk of being linked to related parties. The other Dutch ERDF MAs only use the latter check, as described in Article 72. Risk analyses and risk profiles are also done per project by the MAs, which checks the invoice lists for suppliers and related parties. In Greece, a risk-based methodology is used based on 20 risk factors and updated data derived from the central Management Information System – OPS 2014-2020. 15 of these factors are calculated automatically. In Vlaanderen, the MA carries out risk-based management verifications with the view to minimise the control burden for the beneficiary. Similarly, in both Pomorskie and Warmińsko-Mazurskie, the MAs already use risk-based methods of project or expenditure sampling, and it is expected to further develop the currently applied criteria and procedures (see Box 12).

Box 12: Use of risk-based sampling methods in Warmińsko-Mazurskie

Sampling methods based on risk analysis are used in the ROP Warmińsko-Mazurskie 2014-20 in the case of on-the-spot checks. No changes to this approach are expected, although this depends on the finalised regulation for 2021-27, as well as decisions on the structure of the new OP. Currently, the methodology of selecting a sample of projects for on-the-spot checks is based on the risk analysis of projects implemented under the ROP W-M 2014-20, carried out on the basis of a risk matrix.

Projects are divided into three groups: high, medium and low risk. On the basis of the risk analysis carried out from among the projects implemented under the ROP W-M 2014-20 in a given financial year, the MA selects projects for on-site checks. Due to the specific nature of implemented projects, various factors are used for risk analysis depending on the fund and the department supervising a measure.

The individual risk factors are assigned appropriate weights and scoring criteria. Examples of risk factors are: legal form of the beneficiary, project value, number of projects implemented simultaneously by the beneficiary (under different programmes), project implementation period or irregularities identified by other authorised bodies.

However, with regard to the verification of payment claims, in 2014-20 the MA examines 100 percent of the claims, and it has not yet been decided whether the MA's approach to administrative verifications will change in 2021-27.

Source: IQ-Net fieldwork

7.4 Managing COVID fraud risks

The Coronavirus Response Investment Initiative (CRII) and the Coronavirus Response Investment Initiative Plus (CRII+) introduced a range of flexibility measures to facilitate ESIF spending and management. This included extending the possibility to make use of a non-statistical sampling method by audit authorities, for the accounting year starting on 1 July 2019 and ending on 30 June 2020. An ECA's opinion[25] noted the increased risk associated with the flexibility to use non-statistical sampling methods, which could reduce the reliability of the sample and weaken scrutiny over spending at a time when it is likely to be more exposed to the risk of error and/or fraud.[26]

The CRII/CRII+ initiatives were supplemented with proposals for a REACT-EU instrument and amendments to the 2014-20 Regulations as part of the EU Recovery package, in order to provide a stronger response to the consequences of Covid-19.[27] Again, the ECA's opinion on REACT-EU and the CPR amendments,[28] which included the principles to govern the use of EU funds in emergency situations, emphasised the potential implications for fraud management:

"Significant EU support under emergency measures, together with a relaxation of some procedural requirements, entail an increased risk of irregularities and fraud. All the organisations involved in managing public money should be particularly attentive to these risks."

The views of IQ-Net programme authorities on the implications of COVID investment initiative flexibilities and additional funding through REACT-EU for fraud prevention, risk analysis, control and detection differ. **No significant impact is expected by some IQ-Net authorities** (e.g. AT, Eng, NL, Sco, Vla, W-M), including due to the following factors.

- None of the compliance requirements have been relaxed (Sco).
- The use of CRII flexibilities has been quite measured under the England ERDF OP and the programme will still be subject to the day-to-day contract management work, on-the-spot compliance activity and audit activity. Risks are therefore not considered to be overly high (Eng).
- The monitoring of the projects will remain the same, as the programming of REACT-EU will take place via the current programme structure. The decreasing error rate in recent years and the absence of fraud cases means there is no reason to set up additional control. An important factor is that there is relatively little personnel change in the West MA (NL).
- The Audit Authority already used non-statistical sampling methods before COVID, with the sampling method of the MA thus not expected to change (Vla).
- It should be assumed that all institutions involved in ESIF implementation are still operating correctly and they will not suddenly lower the quality of their activities (this is still assessed by system audits, practically unchanged, possibly with greater emphasis on remote proceedings). It is therefore considered unlikely that the deviation from the random selection of a sample for audits will lead to a failure to ensure the regularity of the underlying operations of the expenditure (W-M).

Where there is recognition of a potentially increased risk, it is considered justified and proportionate (FI, SK). Thus, according to the Antimonopoly Office of the Slovak Republic, the flexibility provided by the CRII and CRII+ has been needed to respond as swiftly as possible to the crisis and in this sense it has been proportionate to the urgency.

At the same time, **various authorities consider that the threat of fraud has increased** (e.g. FR, Wal). For instance, new risk circumstances and areas of fraud emerged that did not occur previously, e.g. relating to: abuse of the fact of *force majeure*; time pressure, simplified and accelerated procurement with zero participation, especially related to healthcare; companies with minimal or zero financial or operational capacity; fraudulent bankruptcies (not) caused by the crisis (e.g. CZ IROP).

The **risk of double funding is also a concern** in some cases (e.g. DK, Wal). For example in DK, the MA foresees potential issues in cases where beneficiaries have received both funding from EU programmes and funding from domestic COVID-19 schemes, which can be considered double funding, with beneficiaries not always being aware of this.

In addition, the fact that it is **not currently possible to carry out on-the-spot visits** due to COVID-19 lock-down and safety requirements may generate increased risk.

COVID-19 and additional funds also may create **additional pressure** on relevant authorities if the management and control systems are maintained within the existing organisational structures and are not strengthened (PT, SK).

In order to respond to these and other related challenges, the following **measures have been introduced.**

- **Simplification**. Some flexibility measures have been introduced such as simplified on-the-spot checks, where photographic evidence has replaced some physical visits and some checks have been postponed to next year (AT). In SK, on-the-spot controls have been replaced with fully electronic communication and provision of documents in order to proceed with payments.

- **Training and capacity-building**. In England, an internal training session was carried out for staff on the potential fraud risk, highlighting areas for contract managers to remind people where fraud might be more likely to happen. The OECD report on best practices to deal with public procurement during COVID-19, as well as exchanges with EC and other countries, have been helpful for the Public Procurement Office of the Slovak Republic to prepare procedures.

- **Measures to avoid double funding**. In Wales, measures were introduced to ensure that when claims are submitted they do not relate to staff who have been furloughed.

- **Revision of penalties policies**. In Slovakia, the Antimonopoly Office amended its prioritisation policy and in specific its calculation on penalties in the time of COVID-19 state of emergency. These changes introduced aggravating circumstances (in the form of increased penalties) in case of infringements taking place during this time.

- **Review of the fraud risk assessment tool**. In England, the annual review of the tool was late this year due to COVID-19, so when it was done, for each risk the MA was able to consider additional issues arising as a result of COVID or CRII and factor these in.

- **Dedicated taskforces**. In order to prevent increases in fraudulent activities related to CRII flexibilities, a 'Taskforce for the fight against frauds and scams' was launched in France. Recommended measures include national coordination for the assessment of the impact of COVID-19 on the systems, a reinforced communication with the private sector, and a general adoption of a risk-based approach.

8 CONCLUSIONS

Fraud risk management of European Structural and Investment Funds has acquired increased salience in recent years in the context of criticism about the effectiveness and misuse of EU funding, a more robust regulatory framework and anti-fraud strategy by the European Commission and proactive efforts by some Member States to tackle fraud and corruption. This paper has examined how fraud risks management is implemented in Cohesion Policy across different contexts across the EU. Drawing on research from IQ-Net countries and regions, it reviewed the key changes in the approaches to fraud risk management in 2014-20 and plans for the future, identified examples of good practice, and explored the factors contributing to the effective and proportionate delivery of fraud risk management systems and measures.

The reinforced emphasis on fraud risk management in 2014-20 has in many cases helped to a promote a more strategic approach to fraud risk management with a stronger role for fraud risk assessment to underpin anti-fraud measures, a clear specification of institutional responsibilities and coordination, along with targeted resources and tools. It has promoted more active discussion, development of new skills, greater transparency and a more integrated approach. New opportunities have been provided by electronic technologies for identifying fraud risk, including increasing use of the Commission's ARACHNE in some (but not all) cases.

There is also strengthened coordination, cooperation and information exchange on fraud management within existing management and controls systems and with anti-fraud coordinating bodies, cooperation with law enforcement bodies, networks, dedicated working groups, workshops, seminars and joint training actions. There is widespread and increasing participation in training and awareness-raising events. Other capacity-building activities include the production of guidance and manuals, and organisation of events for knowledge exchange between MAs and other relevant bodies, including via management meetings, networks for exchange of experience and informal consultations.

While the evolution of fraud risk management is assessed positively overall by most IQ-Net partners, challenges remains and assessments of specific measures are mixed across different countries and regions. There is still scope for improving coordination in many cases through the establishment of central coordination bodies/responsibilities, platforms for information exchange and advice sharing, better cooperation with law-enforcement and prosecution bodies, as well as harmonisation of methodological guidance on fraud risk management. Some authorities face capacity and human resource constraints particularly given the expansion of fraud management responsibilities and requirements, competing tasks/deadlines and time constraints for staff, and insufficient awareness of fraudulent irregularities.

While ARACHNE is a useful tool for preventive searches and information gathering especially on public procurement, it also has limitations: lack of interoperability with other databases and

systems; limitations to the scope for application; identification of a large number of false red flags; lack of consistent use across MAs; complexity and legal constraints. There is scope for improving other capacity-building initiatives as well a need for greater awareness of the existing opportunities among MAs/IBs.

The main lessons drawn from the current for the 2021-27 period are fivefold:

- the need for greater cooperation, harmonisation and interoperability, among the different information systems, institutions and actors;
- simplification, particularly to reduce administrative burden;
- flexibility and proportionality, in the sense of providing scope to adapt the rules and systems to the specific domestic operating and legal contexts;
- enhanced anti-fraud capacity-building, including in terms of resource allocation, training, information and guidance; and
- the need for a greater focus on early detection and prevention, including via enhanced risk assessment mechanisms.

For the 2021-27 period, continuity in fraud risk management approaches is expected in many cases, along with ongoing improvements to IT tools and institutional coordination. While some IQ-Net programme managers do not expect significant implications from the current CRII/CRII+ regulatory flexibilities and additional funding through REACT-EU for fraud prevention, risk analysis, control and detection, others have already seen an increase in fraudulent activities or anticipate additional pressures in the near future. In order to mitigate and address these challenges, new awareness-raising, training and capacity-building actions are foreseen along with revisions of sanctioning policies and simplification of control procedures.

More generally, there are wider necessary preconditions for robust and proactive fraud risk management in the current and future periods, not least in terms of increasing awareness, cultures and mind-sets among managing authorities, implementation bodies and beneficiaries in the face of multiple and often conflicting administrative pressures and priorities to spend funding effectively and efficiently. The scale of fraud risks also varies across countries and regions depending on the relative scale of funding, types of expenditure supported, the quality of institutions and political commitment to tackling fraud.

Notes

[1] European Commission (2020) Statistical evaluation of irregularities reported for 2018: own resources, agriculture, cohesion and fisheries policies, pre-accession and direct expenditure: Part 2, SWD(2020) 160 final, 3.9.2020, European Commission, Brussels.

[2] Algemene Rekenkamer [*Netherlands Court of Audit*] (2020) Rapport bij de Nationale Verklaring 2020. https://www.rekenkamer.nl/publicaties/rapporten/2020/05/20/rapport-bij-de-nationale-verklaring-2020 (accessed 1.10.2020).

[3] https://ec.europa.eu/sfc/sites/sfc2014/files/implem_article125_compendium_en.pdf

[4] Estratégia Antifraude e Avaliação do Risco de Fraude. N.º 04/AD&C/2015. Data: 2015/04/23, https://poise.portugal2020.pt/documents/10180/11008/Norma_04_2015_ADC.pdf/bc4bdc59-737d-478d-8585-fb35788d906f

[5] Central Contact Point for coordinating services for cooperation with OLAF

[6] A service of the Ministry of Finance integrated in the direct administration of the State.

[7] Including: Ministry of Justice, Ministry of Interior, Ministry of Finance / Tax Administration, Customs Administration, Sector for Harmonisation of Internal Audit and Financial Control, Office for Prevention of Money Laundering, Sector for Financial and Budgetary Supervision, Ministry of Economy/ Public Procurement System Directorate, the State Attorney's Office of the Republic of Croatia and the Agency for the Audit of the EU Programme Implementation System.

[8] At the same time, recent efforts by the Central Coordination Body (e.g. their management of the OECD fact-finding mission in Slovakia) and by the National office for OLAF (e.g. their fraud trainings) are considered to be in the right direction.

[9] The Government of the Slovak Republic approved a National Strategy for the Protection of the European Union's Financial Interests in the Slovak Republic in 2015, amended in 2019. One of the steps included in the Action Plan annexed to the Strategy foresees the creation of "*a 'fraud risk management cooperation platform' for interactions in fraud, corruption and irregularity risk management actions (including systematic revision of the existing catalogues of risks) and, where necessary, develop procedures aimed at intensifying controls in the most risky areas (e.g., through methodology guidance)*" by December 2019. Such platform, however, is currently not operational.

[10] 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://www.oecd.org/fr/slovaquie/tackling-fraud-and-corruption-risks-in-the-slovak-republic-6b8da11a-en.htm

[11] HM Government (2019) Guidance on Identifying, Managing and Monitoring Conflicts of Interest within ERDF and ESF;
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/893512/ESIF-GN-1-027_Guidance_on_Identifying_Managing_and_Monitoring_Conflicts_of_Interest_ERDF_and_ESF_v2.pdf

[12] Although the MA assesses resources to be generally sufficient

[13] some IBs organise their own training

[14] Ministry of Economy – IB for OP II (previous IB for OP Research and Innovation)

[15] 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/sfc/sites/sfc2014/files/study-_implem_article125_en-final.pdf

[16] Information about companies, corporations and entrepreneurs; links between them, economic results, financial statements, balance sheets, profit and loss statements, debts. Information is drawn from several public databases. https://foaf.sk/

[17] commercial database of companies and financial data.

[18] https://www.crif.com/products-and-services/risk-management-predictive-analytics/

[19] Note: this might no longer be an issue, and there are plans at the MA to book a new introduction to the ARACHNE tool from the Commission.

[20] Examples of 17 integrity pacts in 11 countries (BG, SK, GR, HU, IT, LV, LT, PL, PT, RO, SI) are available here: https://ec.europa.eu/regional_policy/en/policy/how/improving-investment/integrity-pacts/

[21] Incl information on beneficiary owners (natural persons responsible for legal persons), collective persons or final beneficiaries

[22] i.e. information system which would allow to collect relevant information at the stage of project application and use it e.g. in audits – i.e. information that is relevant both in terms of management and investigation

[23] e.g. by extending the Integrity Pact pilot project in public procurement procedures (Wim)

[24] The draft CPR states that "Management verifications shall be risk-based and proportionate to the risks identified as defined in a risk management strategy"

[25] European Court of Auditors (2020) Opinion No 3/2020 on the proposal 2020/0054(COD) for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 1303/2013 and Regulation (EU) No 1301/2013 as regards specific measures to provide exceptional flexibility for the use of European Structural and Investments Funds in response to the COVID-19 outbreak; https://www.eca.europa.eu/Lists/ECADocuments/OP20_03/OP20_03_EN.pdf

[26] Also see Michie R and Dozhdeva V (2020) When it rains it pours: programme management in a time of crisis. IQ-Net Review Paper 46(1), European Policies Research Centre Delft

[27] Also see Bachtler J, Mendez C and Wishlade F (2020) Will Cohesion Policy recover from COVID? An Initial Assessment, European Regional Policy Research Consortium Paper 20/3, European Policies Research Centre, Glasgow and Delft

[28] European Court of Auditors (2020) Opinion No 4/2020 regarding the proposed REACT-EU regulation and Common Provisions Regulation governing the ESI funds, 14.07.20, Luxembourg