



Council of the
European Union

151053/EU XXVII. GP
Eingelangt am 27/07/23

Brussels, 27 July 2023
(OR. en)

12222/23
ADD 3

GAF 25
FIN 847

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	27 July 2023
To:	Ms Thérèse BLANCHET, Secretary-General of the Council of the European Union
No. Cion doc.:	SWD(2023) 273 final
Subject:	Commission Staff Working Document: Follow-up by Member States to the recommendations of the PIF Report 2021 Accompanying the document "Report from the Commission to the Council and the European Parliament: 34th Annual Report on the protection of the European Union's financial interests and the fight against fraud - 2022"

Delegations will find attached document SWD(2023) 273 final.

Encl.: SWD(2023) 273 final



EUROPEAN
COMMISSION

Brussels, 27.7.2023
SWD(2023) 273 final

COMMISSION STAFF WORKING DOCUMENT

Follow-up by Member States to the recommendations of the PIF Report 2021

Accompanying the document

REPORT FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT

**34th Annual Report on the protection of the European Union's financial interests and
the fight against fraud - 2022**

{COM(2023) 464 final} - {SWD(2023) 272 final} - {SWD(2023) 274 final} -
{SWD(2023) 275 final} - {SWD(2023) 276 final}

TABLE OF CONTENTS

1. Overview of Member States' Replies	7
1.1. PIF Directive Transposition	7
1.2. EPPO Participation	7
1.3. Digitilising the Fight against Fraud	7
1.4. Strengthening Fraud Risk Analysis.....	8
2. Follow-Up by Recommendation.....	9
2.1. Cross-Cutting Measures.....	9
2.1.1. PIF Directive Transposition	9
2.1.2. EPPO Participation	10
2.2. Transparency, Fraud Risk Management, and Digitilising the Fight against Fraud.....	11
2.2.1. Digitilising the Fight against Fraud	11
2.2.2. Strengthening Fraud Risk Analysis.....	12
3. Member States' Replies	18
3.1. Austria (AT).....	18
3.1.1. Correct Transposition of the PIF Directive	18
3.1.2. Participation in the EPPO	19
3.1.3. Digitalising the fight against fraud.....	19
3.1.4. Strengthen fraud risk analysis	19
3.2. Belgium (BE).....	21
3.2.1. Correct Transposition of the PIF Directive	21
3.2.2. Participation in the EPPO	21
3.2.3. Digitilising the fight against fraud	21
3.2.4. Strengthen fraud risk analysis	22
3.3. Bulgaria (BG).....	24
3.3.1. Correct Transposition of the PIF Directive	24
3.3.2. Participation in the EPPO	24
3.3.3. Digitilising the fight against fraud	24
3.3.4. Strengthen fraud risk analysis	25
3.4. Cyprus (CY).....	28
3.4.1. Correct Transposition of the PIF Directive	28
3.4.2. Participation in the EPPO	28
3.4.3. Digitilising the fight against fraud	28
3.4.4. Strengthen fraud risk analysis	28
3.5. Czechia (CZ).....	30
3.5.1. Correct Transposition of the PIF Directive	30
3.5.2. Participation in the EPPO	30

3.5.3.	Digitilising the fight against fraud	30
3.6.	Germany (DE).....	31
3.6.1.	Correct Transposition of the PIF Directive	31
3.6.2.	Participation in the EPPO	31
3.6.3.	Digitilising the fight against fraud	31
3.6.4.	Strengthen fraud risk analysis	32
3.7.	Denmark (DK)	33
3.7.1.	Correct Transposition of the PIF Directive	33
3.7.2.	Participation in the EPPO	33
3.7.3.	Digitilising the fight against fraud	33
3.7.4.	Strengthen fraud risk analysis	33
3.8.	Estonia (EE)	35
3.8.1.	Correct Transposition of the PIF Directive	35
3.8.2.	Participation in the EPPO	35
3.8.3.	Digitilising the fight against fraud	35
3.8.4.	Strengthen fraud risk analysis	35
3.9.	Spain (ES)	37
3.9.1.	Correct Transposition of the PIF Directive	37
3.9.2.	Participation in the EPPO	37
3.9.3.	Digitilising the fight against fraud	37
3.9.4.	Strengthen fraud risk analysis	38
3.10.	Finland (FI)	40
3.10.1.	Correct Transposition of the PIF Directive	40
3.10.2.	Participation in the EPPO	40
3.10.3.	Digitilising the fight against fraud	40
3.10.4.	Strengthen fraud risk analysis	40
3.11.	France (FR)	42
3.11.1.	Correct Transposition of the PIF Directive	42
3.11.2.	Participation in the EPPO	42
3.11.3.	Digitilising the fight against fraud	42
3.11.4.	Strengthen fraud risk analysis	43
3.12.	Greece (GR)	44
3.12.1.	Correct Transposition of the PIF Directive	44
3.12.2.	Participation in the EPPO	44
3.12.3.	Digitilising the fight against fraud	44
3.12.4.	Strengthen fraud risk analysis	44
3.13.	Croatia (HR).....	46

3.13.1.	Correct Transposition of the PIF Directive	46
3.13.2.	Participation in the EPPO	46
3.13.3.	Digitilising the fight against fraud	46
3.13.4.	Strengthen fraud risk analysis	48
3.14.	Hungary (HU)	52
3.14.1.	Correct Transposition of the PIF Directive	52
3.14.2.	Participation in the EPPO	52
3.14.3.	Digitilising the fight against fraud	52
3.14.4.	Strengthen fraud risk analysis	53
3.15.	Ireland (IE).....	54
3.15.1.	Correct Transposition of the PIF Directive	54
3.15.2.	Participation in the EPPO	54
3.15.3.	Digitilising the fight against fraud	54
3.16.	Italy (IT).....	55
3.16.1.	Correct Transposition of the PIF Directive	55
3.16.2.	Participation in the EPPO	55
3.16.3.	Digitilising the fight against fraud	55
3.16.4.	Strengthen fraud risk analysis	56
3.17.	Lithuania (LT).....	59
3.17.1.	Correct Transposition of the PIF Directive	59
3.17.2.	Participation in the EPPO	59
3.17.3.	Digitilising the fight against fraud	59
3.17.4.	Strengthen fraud risk analysis	59
3.18.	Luxemburg (LU).....	61
3.18.1.	Correct Transposition of the PIF Directive	61
3.18.2.	Participation in the EPPO	61
3.18.3.	Digitilising the fight against fraud	61
3.18.4.	Strengthen fraud risk analysis	61
3.19.	Latvia (LV)	63
3.19.1.	Correct Transposition of the PIF Directive	63
3.19.2.	Participation in the EPPO	63
3.19.3.	Digitilising the fight against fraud	63
3.19.4.	Strengthen fraud risk analysis	64
3.20.	Malta (MT).....	65
3.20.1.	Correct Transposition of the PIF Directive	65
3.20.2.	Participation in the EPPO	65
3.20.3.	Digitilising the fight against fraud	65

3.20.4.	Strengthen fraud risk analysis	66
3.21.	Netherlands (NL)	67
3.21.1.	Correct Transposition of the PIF Directive	67
3.21.2.	Participation in the EPPO	67
3.21.3.	Digitilising the fight against fraud	67
3.21.4.	Strengthen fraud risk analysis	68
3.22.	Poland (PL)	69
3.22.1.	Correct Transposition of the PIF Directive	69
3.22.2.	Participation in the EPPO	69
3.22.3.	Digitilising the fight against fraud	69
3.22.4.	Strengthen fraud risk analysis	70
3.23.	Portugal (PT).....	72
3.23.1.	Correct Transposition of the PIF Directive	72
3.23.2.	Participation in the EPPO	72
3.23.3.	Digitilising the fight against fraud	72
3.23.4.	Strengthen fraud risk analysis	72
3.24.	Romania (RO)	74
3.24.1.	Correct Transposition of the PIF Directive	74
3.24.2.	Participation in the EPPO	74
3.24.3.	Digitilising the fight against fraud	74
3.24.4.	Strengthen fraud risk analysis	75
3.25.	Sweden (SE).....	79
3.25.1.	Correct Transposition of the PIF Directive	79
3.25.2.	Participation in the EPPO	79
3.25.3.	Digitilising the fight against fraud	79
3.25.4.	Strengthen fraud risk analysis	80
3.26.	Slovenia (SI)	81
3.26.1.	Correct Transposition of the PIF Directive	81
3.26.2.	Participation in the EPPO	81
3.26.3.	Digitilising the fight against fraud	81
3.26.4.	Strengthen fraud risk analysis	82
3.27.	Slovakia (SK)	85
3.27.1.	Correct Transposition of the PIF Directive	85
3.27.2.	Participation in the EPPO	85
3.27.3.	Digitilising the fight against fraud	85
3.27.4.	Strengthen fraud risk analysis	86

LIST OF ABBREVIATIONS

AFCOS	Anti-Fraud Coordination Service
AFIS	Anti-Fraud Information System
CAP	Common Agricultural Policy
CF	Cohesion Fund
CRMS	Customs Risk Management System
EAGF	European Agricultural Guarantee Fund
EDES	Early Detection and Exclusion System
EPPO	European Public Prosecutors' Office
ERDF	European Regional Development Fund
ESIF	European Structural Investment Funds
ESF	European Social Fund
EU	European Union
FRC	Financial Risks Criteria and Standards Implementing Decision
IMS	Irregularity Management System
IT	Information Technology
MAS	Mutual Assistance System
MFF	Multiannual Financial Framework
NAFS	National Anti-Fraud Strategy
NRA	National Risk Assessment
OLAF	European Anti-Fraud Office
PIF	Protection of the EU's Financial Interests
RRF	Recovery and Resilience Facility
RRP	Recovery and Resilience Plan

1. OVERVIEW OF MEMBER STATES' REPLIES

1.1. PIF Directive Transposition

On 5 July 2017, Directive (EU) 2017/1371 on the fight against fraud against the European Union's (EU) financial interest by means of criminal law (PIF Directive) came into effect. While the deadline for transposing the Directive into domestic law expired on 9 July 2019, the 2021 report on the protection of the EU's financial interests (PIF Report) affirmed that further action was needed to address outstanding compliance issues.

By the end of 2022¹, an infringement procedures for incorrect transposition of the Directive was launched against 18 Member States.

Alongside Czechia, whose infringement procedure was closed in 2022, many of these countries expected to be in full compliance with the PIF Directive in the coming months.

1.2. EPPO Participation

Given the EU's unparalleled recovery plan in the aftermath of the coronavirus health crisis, the 2021 PIF Report highlighted the importance of joining the European Public Prosecutor's Office (EPPO) for investigating and prosecuting fraud against these funds.

In 2022, 22 Member States already participated in the EPPO, with the same five countries as in 2021 abstaining. Again, Denmark and Ireland, which may opt out of freedom, security, and justice policy, as well as Hungary and Poland indicated that they had no intention to join the EPPO. Sweden was still amending its domestic legislation to accommodate membership in the future.

1.3. Digitilising the Fight against Fraud

For the 2021-2027 Multiannual Financial Framework (MFF) and NextGenerationEU, the Commission has additionally put forth specific proposals that are to boost data quality and the interoperability of fund managing information technology (IT) systems, where the budget is implemented under shared management and the Recovery and Resilience Facility (RRF).

As the revision of the Financial Regulation, which would, for instance, oblige Member States to use a single integrated IT system for data-mining and risk-scoring, was ongoing in 2021, the Commission, in 2022, advised Member States to fully exploit the tools at their disposal and develop interoperable solutions with their domestic systems.

Following up on this recommendation revealed that at least one IT system underpins every Member State's anti-fraud efforts. ARACHNE was by far most widely spread, with 21 Member States actively using it, frequently in support of cohesion funds (CF) and RRF. Many used their own dedicated anti-fraud IT tools, often jointly with EU tools, although these tools were rarely interoperable.

Reflecting the Commission's advice, most Member States integrated any of these IT tools into their fight against fraud to enrich data and refine red flags, risk indicators and scores.

¹ As of 10 June 2023, the Commission opened infringement proceedings against 20 Member States for incorrect transposition of the Directive. Of these 20 proceedings, two have been opened in 2023 (Bulgaria and Poland), one has been closed (Czechia) and, in another case (Finland), the Commission decided to send a reasoned opinion. For the remaining 16 (Belgium, Cyprus, Estonia, Greece, Spain, Croatia, Hungary, Luxembourg, Latvia, Malta, The Netherlands, Portugal, Romania, Sweden, Slovenia and Slovakia), the Commission is in the process of assessing the replies to the letters of formal notice it has received from the Member States.

Overall, they assessed the impact of this digitisation as boosting fraud prevention and detection, as well as simplifying administrative procedures. Markedly countries like Finland, which relied on non-EU tools, reported that the potential burden of adjusting domestic data protection law to accommodate the use of, for example, ARACHNE was keeping them from doing so.

1.4. Strengthening Fraud Risk Analysis

Under the 2021-2027 MFF and NextGenerationEU, the 2021 PIF Report more broadly, too, recommended to proactively approach the protection of the EU's financial interests. Such an approach would encompass using data from all available sources, analysing the data and exchanging information, including with law enforcement authorities and the Commission to specify emerging risks and fraud trends timely. Member States should further act on information provided by the Commission and feedback promptly on the actions taken in response.

In 2022, 14 Member States considered that they had implemented this recommendation in full, reiterated their proactive approach to combatting fraud against the EU budget and presented recent initiatives. On the revenue side, these Member States highlighted the Financial Risks Criteria and Standards (FRC) Implementing Decision, supporting national and EU level IT Tools such as the Customs Risk Management System (CRMS)² and the Anti-Fraud Information System (AFIS), which helped tax and customs authorities to mine and enrich data from a variety of sources and to exchange data among Member States and with the EU institutions. On the expenditure side, Member States highlighted certain context-specific fraud risk management systems developed by EU fund managing authorities, as well as top-level coordination, IT tools like ARACHNE, and dedicated trainings.

Member States that indicated only partial compliance (12) with the advice to strengthen their fraud risk analyses reported similar measures, but had, to date, not implemented these for revenue and expenditure. Sometimes, as was the case for Germany, the extent to which this recommendation was implemented varied by governance level and amongst states due to the Member State's competence distribution.

Only Sweden is still to implement this recommendation, while Ireland and Czechia did not report on it.

In this context, it is also noteworthy that Member States such as Finland, which had only partially implemented the Commission recommendation, pointed to a high burden stemming from administering and legislatively accommodating tools such as ARACHNE into its domestic data protection framework.

² CRMS is a European electronic system for customs, financed by the EU Customs Programme. CRMS2, the new release of the system, started to operate on 1 January 2022

2. FOLLOW-UP BY RECOMMENDATION

2.1. Cross-Cutting Measures

2.1.1. PIF Directive Transposition

On the correct transposition of the PIF Directive, the Commission asked Member States the following questions:

Q.1. Has the Commission initiated infringement procedures against you for the incorrect transposition of the PIF Directive?

If YES, have you taken remedial action to modify national legislation?

If YES, by when do you expect to complete the modification of national legislation to transpose correctly the PIF Directive?

By the end of 2022³, an infringement procedures for incorrect transposition of the Directive was launched against 18 Member States.

Alongside Czechia, whose infringement procedure was closed in 2022, many of these countries expected to be in full compliance with the PIF Directive in the coming months.

After sufficient adjustments, the procedure concerning **Austria** closed in 2022. On November 6, 2019, the Austrian Federal Ministries of Justice and Finance first contended September's formal notice, stating that domestic law mostly complied with EU requirements. On November 19, Austria then referred to an ongoing government proposal to amend accordingly its criminal law. The Member State finally provided additional comments on December 30, 2021, when said Act had been adopted, asking the Commission to end the procedure, which was indeed closed on May 19, 2022.

In 2022, the infringement procedure against **Cyprus** for failing to transpose the PIF Directive was still ongoing. Back then, the draft law that is to remedy all launched infringements was going to be legally scrutinised and submitted for adoption when the House of Representatives reconvened after Cypriot presidential election on February 5 and 12, 2023.

On January 24, 2022, **Spain** responded to the European Commission's letter of formal notice, which objected to the Member State's failure to transpose the PIF Directive. In that, the Ministry of Justice's Technical Secretary General justified the transposition of all articles concerned, namely, Articles 4(2)(a), 4(2)(b), 7(1), and 7(3). Spain, however, has not yet received an answer.

Following the opening of infringement procedure, **Greece** reported that it had responded to the Commission.

Throughout 2021 and 2022, **Latvia** modified its domestic law to remedy all infringements to which the European Commission had objected on December 2, 2021. After reporting that all violations in its Criminal Law, Law on Administrative Penalties for Offences in Administration, Public Order, and

³ As of 10 June 2023, the Commission opened infringement proceedings against 20 Member States for incorrect transposition of the Directive. Of these 20 proceedings, two have been opened in 2023 (Bulgaria and Poland), one has been closed (Czechia) and, in another case (Finland), the Commission decided to send a reasoned opinion. For the remaining 16 (Belgium, Cyprus, Estonia, Greece, Spain, Croatia, Hungary, Luxembourg, Latvia, Malta, The Netherlands, Portugal, Romania, Sweden, Slovenia and Slovakia), the Commission is in the process of assessing the replies to the letters of formal notice it has received from the Member States.

Use of the Official Language, and the Taxes and Fees Law had been corrected, Latvia had not received an answer yet.

Malta, too, reported that it had taken remedial action that addressed all launched infringements. In 2022, these changes were tabled in parliament and expected to close swiftly, whereafter Malta would report to the Commission.

Sweden, in parallel, appointed an Inquiry Commission to evaluate its alleged failure to correctly incorporate the PIF Directive (Articles 3(2)(d)(iii), 5(2)) into domestic law. By August 31, 2023, this Commission will report on possible relief actions targeting Articles 3(2)(d)(i) and 3(2)(d)(iii). To remedy infringements of Article 5(2), the Swedish government has proposed that any attempt to commit subsidy abuse or gross subsidy abuse be criminalised. These amendments will like enter into force on June 1, 2023.

When reporting, **Slovenia** had taken action to remedy only part of the PIF Directive infringements objected to by the European Commission. Effective in February 2023, the Member State amended solely its Criminal Code, more specifically, the definition of official persons. It contended the Commission's remaining comments in a reply to the letter of formal notice, arguing that Slovenia believed its regulation was fit for purpose and further changes were unnecessary. The Commission response was still pending.

Finally, **Slovakia** fully complied with the Commission's formal notice, aligning domestic law with the PIF Directive effectively by January 1, 2024.

2.1.2. EPPO Participation

Regarding Member States' participation in the EPPO, the Commission reiterated its call for those that have not yet joined it to do so. It further advised Member States that already participate in the EPPO to ensure that the prosecutor is able to exercise all powers bestowed upon it by its founding Regulation.

The Commission probed for progress with the following questions:

Q.1. Are you already participating in the EPPO?

If NO, are there plans to join the EPPO in the short-medium term?

If YES, when do you expect to finalise the procedure?

Table 2: Overview of present and planned EPPO participation across Member States.

Member State																										
AT	BE	BG	CY	CZ	DE	DK	EE	ES	FI	FR	GR	HR	HU	IE	IT	LV	LT	LU	MT	NL	PL	PT	RO	SE	SI	SK
YES																										
NO, with plan																										
NO, without plan																										

In 2022, 22 Member States already participated in the EPPO. Of the five Member States that did not participate, Denmark and Ireland, both of which may opt out of freedom, security, and justice policy, as well as Hungary and Poland reported no intention to join. Sweden, by contrast, argued that its

government is currently working on a legislative proposal that would allow the country to join the EPPO as soon as possible, assuming that the Parliament endorses it.

2.2. Transparency, Fraud Risk Management, and Digitilising the Fight against Fraud

2.2.1. Digitilising the Fight against Fraud

As the Financial Regulation's revision is ongoing, the Commission invited Member States to make full use of the tools at their disposal (ARACHNE, EDES, and IMS). It also encouraged the development of interoperable solutions with national systems to fully realise their potential.

On Digitilising the fight against fraud, the Commission followed-up with the following questions:

Q.1. Are you using any of the following IT systems in your fight against fraud, including ARACHNE, EDES, IMS, others, or national dedicated anti-fraud IT tools?

Q.2. Has any interoperability been developed between EU IT tools and national IT tools?

If YES, with which tool?

Q.4. To what end?

Q.5. How is digitalisation influencing the fight against fraud?

For any impact selected, can you provide any quantification?

Table 3: Overview of IT systems used by Member States in their fight against fraud and their interoperability (int.).

System	Member State																			
	AT	BE	BG	CY	CZ	DE	DK	EE	ES	FI	FR	GR	HR	HU	IE	IT	LT	LU	LV	MT
Arachne																				
EDES																				
IMS																				
Other																				
National																				
Int.																				

ARACHNE		National	
EDES		NO	
IMS			
Other			

Markedly, every Member State reported that at least one IT system underpinned their anti-fraud efforts. ARACHNE was by far most widely spread, with 21 Member States actively using it, except Austria, Germany, Denmark, Finland, Ireland, and Sweden. It most frequently supported cohesion funds (13), 6 times all programmes⁴ and 7 times a limited number⁵. Otherwise, ARACHNE was used on 10 accounts in administering the RRF⁶. Estonia, Croatia, and Romania used ARACHNE for rural development funds. In Czechia, Bulgaria, and Italy, this tool aided anti-fraud action across all EU funds and programmes.

⁴ Croatia, Hungary, Luxembourg, Malta, Romania, Slovenia

⁵ Belgium, Estonia, France, Latvia, Netherlands, Portugal, Spain

⁶ Belgium, Cyprus, Greece, Hungary, Luxembourg, Malta, Netherlands, Poland, Portugal

EDES was only used by 6 Member States, while IMS and other tools were reportedly common amongst 12 and 13 Member States respectively. 14 Member States used their own dedicated anti-fraud IT tools, often jointly with EU counterparts, although they were only interoperable in 6 instances.

Overall, 10 Member States confirmed this system quality. Italy and Slovakia were outliers in this regard. Italy used all EU tools and a national tool, which were interoperable with ARACHNE, IMS, EDES, and other systems. Slovakia noted that it ran all EU, a national, and other anti-fraud tools compatibly with IMS, ARACHNE, and others.

In contrast to Austria, Sweden and Finland relied exclusively on national dedicated anti-fraud IT tools, which were also not interoperable with EU tools.

The reason for integrating any of the above IT tools into the fight against fraud was most frequently data enrichment (12)⁷, followed by the refinement of red flags, risk indicators and scores (6)⁸, the introduction of red flags, risk indicators (5)⁹, and, finally, streamlining and automation of irregularities reporting (1)¹⁰. Notably, only 12 Member States provided insights to their motivation.

All Member States but Greece, Ireland, and Sweden revealed how this digitisation impacted their anti-fraud efforts. All Member States (23), except Cyprus, indicated that using IT tools fostered fraud prevention as opposed to decreasing (1) it. Slovenia reported both. Increased (19)¹¹ rather than decreased fraud detection (2)¹² and reducing or simplifying administrative procedures (18)¹³ were similarly common. Few Member States (8)¹⁴ reported that these tools bore a higher administrative burden.

2.2.2. Strengthening Fraud Risk Analysis

To identify and address emerging risks and fraud trends, the Commission urged Member States to use data from all available sources, analyse the data, and exchange information on them, including with enforcement authorities and the Commission. It also reminded Member States to act upon the information provided by the Commission in this and other strategic analyses as well as targeted reports and promptly feedback on the actions they take to help monitor fraud risks and trends.

This recommendation, the Commission followed-up with this question:

Q.1. Have you implemented the recommendation?

If YES fully, then please describe the process, share any specific findings if possible, and make a distinction between revenue and expenditure areas.

If YES partially, then please explain why you think it was a partial implementation and why a full implementation was not possible. Here, too, please distinguish between revenue and expenditure areas.

If NO, please explain why.

⁷ Austria, Belgium, Bulgaria, Czechia, Italy, Latvia, Lithuania, Luxembourg, Malta, Romania, Slovenia, Slovakia

⁸ Austria, Czechia, Italy, Malta, Romania, Slovakia

⁹ Austria, Czechia, Italy, Malta, Slovenia

¹⁰ Slovakia

¹¹ Belgium, Bulgaria, Croatia, Cyprus, Czechia, Denmark, Estonia, Hungary, Italy, Latvia, Lithuania, Malta, Netherlands, Poland, Portugal, Romania, Slovenia, Slovakia, Spain

¹² Romania, Slovenia

¹³ Austria, Belgium, Bulgaria, Croatia, Cyprus, Czechia, Estonia, Germany, Italy, Latvia, Lithuania, Malta, Poland, Portugal, Romania, Slovenia, Slovakia, Spain

¹⁴ Belgium, Denmark, Finland, France, Germany, Luxembourg, Netherlands, Spain

Table 4: Overview of response to the advice to strengthen fraud risk analysis by Member States.

Member State																				
AT	BE	BG	CY	CZ	DE	DK	EE	ES	FI	FR	GR	HR	HU	IE	IT	LT	LU	LV	MT	NL

YES, fully		NA
YES, partially		
NO		

Most Member States implemented the Commission's advice to bulk up their fraud risk analyses. 14 did so fully and 12 in part. Only Sweden did not follow this recommendation at all, while Ireland and Czechia did not report on it.

Austria focused on revenue from customs, where the Finance Ministry's anti-fraud department defines risk areas, develops countermeasures, and draws up control strategies, in line with the EU risk management rules.

Belgium, too, has committed fully to this recommendation across, especially on the expenditure side, including European Regional Development Fund (ERDF) and RRF funds in Wallonia, and ERDF funds in Flanders as well as the Flemish government's department for agriculture and fisheries. In Flanders, the General Regulation imposes upon the ERDF funds proportionate anti-fraud measures, which the Audit Authority assesses at the implementation stage. This system has been rated as functional. Within the new programming period, beginning on January 1, 2023, the Flemish Department of Agriculture and Fisheries re-examined fraud risks, which it then integrated into all related grant measures and processes.

In **Bulgaria**, numerous bodies protecting the EU budget's revenue and expenditure strengthened their fraud risk analyses, following the Commission's advice. The Customs Agency drew on a variety of data sources. As the certifying authority, the National Fund Directorate, which oversees managing authorities' procedural conduct and control activities, for example, now widely uses ARACHNE to perform its checks. The Bulgarian Audit of EU Funds Agency, throughout its auditing activities, reportedly carried out checks to identify fraud indicators, analysed and presents cases in its annual control report for each programme, notified competent authorities, and regularly reviewed related Commission guidelines. The Public Procurement Agency reviewed and analysed data from various sources like the European Anti-Fraud Office (OLAF) and the World Bank, assigning risk weights used in the random selection of control procedures. And, finally, Bulgaria's State Agency for National Security, the Ministry of Innovation and Growth, and the Ministry of the Interior, signed an agreement to facilitate information and data exchanges on emerging fraud risks.

Cyprus equally followed through on the fourth 2021 PIF Report recommendation. On revenue focused fraud risk analyses, especially customs and excise duties, Cyprus reported that it adhered to Commission advice. Accordingly, it processed all information received through the CRSM2 and AFIS, as well as acted on it. Financial risks, in particular, were examined closely, using the common criteria for combatting fraud. Accounting for both measures, risk information forms, and OLAF statistics the Cypriot Post Control and Audit Department then planned post-control audit, clearly following a risk based approach.

The Member State further reported five steps toward wholly strengthening its fraud risk analysis in the expenditure of EU RRF funds. Firstly, concerning its Recovery and Resilience Plan (RRP), Cyprus began to use the Commission's fraud risk assessment tool. The tool covers an array of data on basic procedures like application selection, quantifying fraud risks, and weighing existing controls and the value of possible additions. To support this process, Cyprus, secondly, relied on the

ARACHNE tool, which is risk focused. Since successful, the country considers applying this approach also for cohesion policy. Thirdly, Cyprus established an independent anti-corruption authority, which will coordinate anti-corruption actions across public services, the public and private sector. In that, it could also improve the coherence of fraud risk analyses through, for example, information exchanges. Fourthly, the Member State now follows guidelines that align domestic and EU public procurement, prevention and detection, corruption and conflict of interest policy. And, fifthly, Cyprus amended two regulatory administrative acts to grant all domestic and EU control bodies access to beneficial ownership databases.

To strengthen fraud risk analysis, in particular **France's** Agency for Territorial Cohesion regularly hosted a working group that brings together EU fund managing authorities, harmonising existing arrangements for the prevention, detection, and reporting of fraud. Using various databases alongside or instead of ARACHNE, these authorities exchanged information in this channel to prevent double funding. It has further distributed Commission information notes and practical guides on red flags amongst its members. And, lastly, the working group has issued a risk analysis focused training catalogue, in some of which the EPPO participates to illustrate its support functions.

Greece enhanced fraud risk analyses of customs and excise duties as well as European Agricultural Guarantee Fund (EAGF) and RRF spending, affirming a proactive approach to protect the EU's financial interests. Greece emphasised that its customs controls followed Article 46 of the Union Customs Code, used all available information, especially from OLAF's mutual assistance messages and RIFs, and created corresponding risk profiles. Further, in the Member State, the Ministry for Rural Development and Division for Financial Control and Audit and Cooperative Affairs controls direct and indirect beneficiaries and debtors of the EAGF *ex post*. These controls' fraud risk sensitivity has been improved by integrating specific risks and risk values, all relevant data, and information from the Commission throughout the selection of undertakings, their control plan and scrutiny. To protect better the RRF from fraud, Greece has further adopted two legislative measures. Decision 129397/13-09-2022 was made by the RRF Agency's Governor. It set up a fraud risk assessment team and designated an officer at the agency as responsible for fraud issues. With Decision 135896/21-09-2022, the agency's governor also approved a new risk assessment methodology for the *ex-ante* check for conflicts of interest when awarding public contracts.

With contributions from its anti-fraud coordination service (AFCOS), Agency for Territorial Cohesion, Ministry of Justice, and the Ministry of Education, **Italy** has fully executed the present advice with a focus on expenditure. The Italian AFCOS' fraud risk analyses are reportedly underpinned by IT tools that run on a large volume of data from various sources, such as the Anti-Fraud Platform. It further coordinates and implements the country's national anti-fraud strategy (NAFS), including though a new network of anti-fraud contact points. These contact points coordinate specifically fraud risk, conflict of interests and double funding assessments of Italy's RRP. The Agency for Territorial Cohesion, on the other hand, relies on ARACHNE for on-the-spot checks and to disseminate information on audit findings. It also issued new guidelines on using ARACHNE throughout the management and control of programmes under the ERDF. The Ministry of Justice has adjusted legislation to fully accommodate the EPPO in the fight against fraud. And the Ministry of Education uses all tools available to monitor fraud risks to its national school operational programme.

Lithuania's effort to strengthen fraud risk analysis has been trifold and horizontal. Competence-based cooperation with the EPPO, the comprehensive use of ARACHNE, and developing an evaluation methodology for criminal threats to the financial system, the Member State ensures that fraud risks and trends are accounted for.

Latvia, too, generally bulked up its analysis of fraud risks to EU budget inflows and outflows. EU funds managing authorities and bodies now carry out regular risk assessments, using all available data, IT tools and information, including that provided by the Commission, to take timely preventative

actions against fraud and corruption. Aiming at revenues in addition to expenditure, the Latvian AFCOS disseminated all information from the Commission to its network through a dedicated platform, and has developed an IT tool that helps monitor risks and trends.

Luxembourg reiterated its proactive approach to fraud risk detection across EU revenue and expenditure streams, which evolved around information sharing and trainings in 2022.

Poland, too, reaffirmed its proactive approach to protecting the EU's financial interests comprehensively. On the revenue side, Poland has focused facilitating information exchanges with the Commission and Member States via CRMS2 and AFIS, which anchor the analysis of risks, their identification, and feedback on actions taken based on the information received. Generally, analyses of fraud risks to budget outflows are supported by an array of tools, mechanisms, cooperation agreements, and reporting measures. The Signal system, for example, facilitates an information exchange on risky entities amongst CF managing authorities, alongside newly digitised auditing processes, ARACHNE, and the SL2014 application. An agreement between Poland's public prosecutor and the minister for regional development enables regular exchanges of beneficiaries' data. Annual reports on fraud risks to agricultural funds, which identify risks, assess and introduce new control mechanisms, prevent that they are compromised.

Romania reaffirmed its full commitment the fourth recommendation on the revenue and expenditure side. In 2022, the Romanian customs authority was subordinated to its ministry of finance, adding layers to fraud risk analysis of inflows. The agency incorporated the FRC Decision into its risk management system, which is supported by CRMS and AFIS, as well as a national IT application for specific activities. At the central government level, Romania reported further a mutual assistance coordinating body, and regular exchanges with Romanian law enforcement. On part of expenditures, Romania pointed to the contribution of the competitiveness, large infrastructure, and technical assistance operating programmes' managing authorities as well as an RRF specific fraud risk analysis structure. Accordingly, the Directorate General for Smart Growth and Digitalisation carried out a fraud risk assessment in 2022. Romania further closely monitors irregularities until they are resolved, has created several level of checks, including internal operational procedures, and actively uses ARACHNE in this domain, too. The Directorate-General for Sustainable Development, at the same time, has also carried out a fraud risk assessments, while the technical assistance managing team used the ARACHNE tool to complement its risk analysis activities. The RRF, finally, had its own administrative, organisation, and operational measures such as a dedicated IT system that runs on several national institutions' databases on beneficiaries, an prevention, monitoring, and recovery oriented procedures.

Slovenia similarly reaffirmed its commitment to protecting EU budget revenue and expenditure stream through thorough risk analyses. The Member State emphasised the proactive role of customs and VAT relevant authorities. Accordingly, fraud risk data exchanges took place at EU level, as they were facilitated by systems such as CRMS and AFIS to create risk profiles, apply checks preceding release into free circulation, ex-post checks, and inspections. This information was also forwarded internally. AFIS made reportedly the biggest difference by underpinning several databases and tools, used, for example, to create risk profiles for undervalued goods, tracking container ships, and checking the legitimacy of declaring companies. Slovenia also highlighted information exchanges with OLAF and mutual assistance amongst Member States using a Eurifisc tool. On part of cohesion policy and the RRF, Slovenia pointed to the use of ARACHNE, national databases, regular reporting, on the one hand, and strategic foresight, cooperation with the EPPO, and trainings, on the other hand.

Finally, **Slovakia** illustrated its proactive approach to thoroughly protecting the EU's financial interests. On the revenue side, the Member State highlighted data analyses using various sources to identify trends in the circumvention of customs regulations, as well as information exchanges internally and with OLAF. For expenditure fraud risk analyses, it pointed to the contributions of

various EU fund managing authorities. Its government, for example, had an OLAF dedicated department that ensured top level coordination of various anti-fraud efforts and distributed information on emerging risks and trainings in to the AFCOS network, ensuring also that national authorities use EU and national databases, exchange information and provide mutual assistance. Otherwise, Slovakia was keen to follow EU recommendations, measures, and action plans, and developed internal fraud prevention guidelines.

In **Germany**, whether expenditure fraud risk analyses had been strengthened varied by level of governance and amongst states. The Federal Ministry of Labour and Social Affairs exploits all available resources to fight fraud, by encouraging European Social Fund (ESF) managing authorities to self-asses and exchange information. In Rhineland-Palatinate, North-Rhine Westphalia, and Mecklenburg-Vorpommern, the ERDF managing authorities only partially followed this recommendation, due to limited resources. For example, limited resources restrict Rhineland-Palatinate's capacity to using reports from the Regional Court of Auditors, the European Court of Auditors and the ERDF audit authority to identify fraud risks. Other ministries, like the Federal Ministry for Food and Agriculture, and states, such as Bavaria, did not take action after the Commission's advice to boost fraud risk analysis, since they already had established procedures that ensure the timely detection of fraud risks and trends.

Denmark, too, implemented the fourth 2021 PIF Report recommendation only in part, focusing on customs and agricultural, cohesion, and fisheries funds. Accordingly, Denmark reported that its Customs Agency used data from all available resources, which it analysed, and acted upon, even if not in every instance. At the Danish Agricultural Agency, on the other hand, a statutory risk assessment will be integrated into the accreditation conditions for authorities that disburse funds under the Common Agricultural Policy. The Danish Business Authority currently investigates how ARACHNE could complement existing controls. And, finally, fisheries funds managing authorities use IMS to report irregularities to the Commission.

Estonia has comprehensively boosted fraud risk analyses in EU budget revenue streams, and partially in expenditure. The Estonian Customs Agency has created an IT tool that enables its use of Theseus across commodities more broadly, exploiting fully available sources and data to better protect the EU's financial interests. On the expenditure side, the possibility of using ARACHNE for risk assessments across the 2021 – 2027 European Structural Investment Funds (ESIF) programming period is being assessed for deployment in 2023; in agriculture, ARACHNE is used as an additional source for risk assessment.

Similarly to Estonia, **Spain**, in 2022, implemented this final recommendation fully on the revenue and partially on the expenditure side. Its State Tax Administration Agency, which governs Spain's tax and customs system, runs its risk analyses on a consolidated database, using all available sources, including internal data bases, open source information, and data from OLAF, and exchanging information with law enforcement authorities and other Member States. In ETC, ESF, and the RRF, such a system is not yet fully in place, due to unclearly distributed competences and resource and IT tool differences. However, Spain insisted that the recommendation's adoption is progressing. In the ETC, the use of shared databases is already wide spread, and in managing the ESF and RRF authorities have drawn up corresponding plans and made organisational changes.

Finland, too, has thoroughly improved its fraud risk analyses of EU budget inflows, but incompletely altered procedures surrounding spending. In 2022, Finnish Customs developed and fully automated data processing for risk detection, using official sources like CRM2, AFIS, and the Mutual Assistance System (MAS). On part of expenditure, especially the RRF, data analysis has been improved by completing data bases, obliging the managing authorities to update them regularly, making this data available to control and inspection authorities, controlling and auditing the data, and recording these activities' results. Using ARACHNE to support this process remains, however, undecided upon as

resource constraints limit Finland's ability to accommodate the tool into its data protection framework and administration.

In **Croatia**, progress was made exclusively on improving fraud risk analyses of expenditures, with contributions from the Ministry of Regional Development, the Ministry of Agriculture, and the EU Programmes Implementation System Audit Agency. The Ministry of Regional Development has implemented the Commission's recommendation most comprehensively. Regular staff trainings, the obligation to forward acquired knowledge, workshops for analysts, monitoring and the dissemination of relevant data and documents, and ARACHNE allow fraud risk assessments of European Structural Investment funds to be followed up with appropriate measures, also through cooperation with OLAF and the EU's judicial bodies. Croatia's audit authority has similarly comprehensively improved fraud risk analyses related to all EU funds, but the RRF in particular. Actions revolved mostly around awareness raising amongst and training staff, as well strengthening Croatia's AFCOS network and system. Efforts by the Ministry of Agriculture, by contrast, remain incomplete, with data types and sources being varied, collection and processing being supported by the Integrated Administration and Control System, the Area Monitoring System, and ARACHNE, and information exchanges running smoothly, but information management IT systems for Common Agricultural Policy (CAP) funds needing to be updated.

Hungary primarily enhanced fraud risk analyses of EU revenue and expenditure streams by realising the Commission's FRC Decision and Guidance and continuing to develop its domestic IT system, both of which were incomplete processes. Following the Commission's advice, Hungary, in 2022, already made analysis and profiling more confident, and, using the National Tax and Customs Administration's risk management system, conducted real time risk analyses and timely interventions. Hungary's FAIR system, which supports risk analyses of expenditure streams, was given fraud prevention functions, its sources were broadened, credibility improved and the administrative burden on beneficiaries reduced.

Malta's Internal Audits and Investigations Department, for the first time, published a comprehensive National Risk Assessment (NRA) on Fraud and Corruption linked to public funds, which covers also funds that Malta is required to manage under its international obligations. The NRA therefore marks an important step towards improving the Member State's fraud risk response, including with respect to EU funds. As it was collaboratively produced, involving all members of the co-ordinating committee, the report facilitated information exchanges, in particular.

In 2022, the **Netherlands** used ARACHNE to gain an overview of fraud risks that permeate expenditure, and progressively improved their approach to their anticipation in EU budget revenue. To the latter end, the Dutch internal audit offered an opinion on fraud risks, which found them to be adequately managed by ministries, and initiated the formation of a Security and Integrity Office dedicated to fraud risks and necessary follow-up measures.

Portugal reported that it had thoroughly strengthened its analytical approach to fraud risks to tax and customs duties, but recently revised its overarching NAFS, including a five-year action plan that sets out concrete fraud risk analysis measures in the expenditure domain. Only after 2022, would the latter measures be realised.

While **Ireland** and **Czechia** abstained from following-up on their risk analyses, **Sweden** is the Member State that indicated that it had not realised the Commission's recommendation to bulk up this capacity. Its response suggests that although Sweden proactively protects the EU's financial interests, for instance, by monitoring OLAF advice and reports, domestic legislation prevents the use of fraud relevant data outside the judicial system. In December, 2021, Sweden did, however, report that it had initiated an inquiry into how it could more effectively, efficiently, and legally secure its management of EU funds.

3. MEMBER STATES' REPLIES

3.1. Austria (AT)

3.1.1. Correct Transposition of the PIF Directive

Q.1. Has the Commission initiated infringement procedures against you for the incorrect transposition of the PIF Directive?

☒ YES

*On 19 September 2019, the European Commission sent a letter of formal notice to Austria, objecting to the failure to transpose Directive (EU) 2017/1371 of the European Parliament and of the Council of 5 July 2017 on the fight against fraud to the Union's financial interests by means of criminal law (the '**PIF Directive**'); infringement case No 2019/0258). On 6 November 2019, the Austrian Federal Ministry of Justice (BMJ) issued a partial notification, stating that the vast majority of the requirements contained in the PIF Directive had been complied with by provisions in place and set out in the Austrian Criminal Code, the Code of Criminal Procedure and the Act on the Criminal Liability of Associations. According to the information available to the BMJ, a separate notification was also issued by the Federal Ministry of Finance (concerning implementing legislation regarding the Austrian Financial Offences Act).*

In addition, on 19 November 2021, Austria submitted a series of observations referring to the existing government proposal for a Federal Act amending the Criminal Code, the Act on the Federal Office for the Prevention of Corruption and the Fight against Corruption and the 1975 Code of Criminal Procedure to implement the Directive on the fight against fraud to the Union's financial interests by means of criminal law. Austria also provided additional comments on 30 December 2021, in which reference was made to the notification of the Act adopted in the meantime and which came into force on 28 December 2019 (Federal Law Gazette I No 111/2019). The Commission was asked to close the infringement case.

Following a decision by the Commission on 19 May 2022, infringement proceedings in case No 2019/0258 for failing to transpose the PIF Directive were closed.

*It should be noted that the infringement proceedings in question were based on the failure to transpose, whereas the questions contained in the questionnaire sent under point 2.1.2 refer to 'incorrect transposition'. **It is unclear to the BMJ whether infringement case No 2010/0258 is actually addressed by the questions raised under point 2.1.** If so, the answers to Question 2.1.2 would be as follows:*

Q1: YES

Q2: YES, for all launched infringements

Q 3: Infringement proceedings were closed on 19 May 2022.

It should also be noted that the BMJ was also contacted by the Commission on substantive issues relating to the implementation of the PIF Directive. To date, that exchange has been exclusively via e-mail. We have yet to receive a response from the Commission to our e-mail of 19 October 2022. Therefore, as we understand it, no infringement proceedings are currently open against Austria in connection with the PIF Directive.

Q.2. For the Member States having replied yes. Have you taken remedial action to modify national legislation?

☒ YES, for all launched infringements

Q.3. For the Member States having replied yes. By when do you expect to complete the modification of national legislation to correctly transpose the PIF Directive?

Infringement proceedings were closed on 19 May 2022.

3.1.2. Participation in the EPPO

Q.1. Are you already participating in the EPPO?

☒ YES

3.1.3. Digitalising the fight against fraud

Q.1. Are you using any of the following IT systems in your fight against fraud?

☒ National dedicated anti-fraud IT tools (*In the field of customs revenue*)

Q.2. Has any interoperability been developed between EU IT tools and national IT tools?

☒ YES

Q.3. If yes, with which tool?

☒ other (specify)

EU systems ICS (Import Control System) CRMS.

Q.4. To what end?

☒ Data enrichment

☒ Introduce new red flags/risk indicators

☒ Fine tune/refine red flags/risk indicators/risk scoring

Q.5. How is digitalisation influencing the fight against fraud?

☒ Increasing prevention

☒ Reducing/simplifying administrative procedures

Q.6. For any impact selected, can you provide any quantification?

No, but the purpose of digitalisation is to ensure targeted controls based on electronic data analysis in order to avoid 'false hits'.

3.1.4. Strengthen fraud risk analysis

Q.1. Have you implemented the recommendation?

☒ YES, fully

If you implemented fully the recommendation, can you please describe how you have done it? Can you share any specific findings? Please make a distinction between revenue and expenditure areas.

In the field of customs revenue:

In the area of customs, the EU risk management rules developed jointly by the European Commission and Member States are implemented nationally based on the EU Risk Management Strategy and Action Plan. The customs administrations in Member States are required by EU law to transpose measures identified as recommendations into national law. In Austria, the anti-fraud department of the Ministry of Finance defines the risk areas, develops countermeasures and draws up appropriate control strategies for individual risk areas.

3.2. Belgium (BE)

3.2.1. Correct Transposition of the PIF Directive

Q.1. Has the Commission initiated infringement procedures against you for the incorrect transposition of the PIF Directive?

☒ YES *FPS Finances (General Administration of Customs and Excise) and FPS Justice*

Q.2. For the Member States having replied yes. Have you taken remedial action to modify national legislation?

☒ NO *FPS Finances (General Administration of Customs and Excise) and FPS Justice*

3.2.2. Participation in the EPPO

Q.1. Are you already participating in the EPPO?

☒ YES *ERDF and RRF Wallonia, Department of Agriculture and Fisheries, FPS Finances (General Administration of Customs and Excise) and FPS Justice*

3.2.3. Digitilising the fight against fraud

Q.1. Are you using any of the following IT systems in your fight against fraud?

- ☒ ARACHNE *ERDF and RRF Wallonia, ERDF and RRF Brussels, ERDF Flanders*
- ☒ Cohesion (not all programmes) *ERDF and RRF Wallonia, ERDF and RRF Brussels*
- ☒ Recovery and Resilience Facility *ERDF and RRF Wallonia*
- ☒ other (specify) *ERDF and RRF Wallonia*

Q.2. Has any interoperability been developed between EU IT tools and national IT tools?

☒ NO *ERDF and RRF Wallonia, ERDF and RRF Brussels, Department of Agriculture and Fisheries, ERDF Flanders*

Q.4. To what end?

- ☒ Data enrichment *ERDF and RRF Brussels*
- ☐ Introduce new red flags/risk indicators *ERDF and RRF Brussels*

Q.5. How is digitalisation influencing the fight against fraud?

- ☒ Increasing prevention *ERDF and RRF Wallonia, ERDF and RRF Brussels, Department of Agriculture and Fisheries*
- ☒ Increasing detection *ERDF and RRF Wallonia, ERDF and RRF Brussels, Department of Agriculture and Fisheries*
- ☒ Increasing administrative burden *ERDF and RRF Wallonia, ERDF and RRF Brussels*
- ☒ Reducing/simplifying administrative procedures *ERDF and RRF Wallonia*

Q.6. For any impact selected, can you provide any quantification?

ERDF and RRF Wallonia: In terms of prevention: However it is impossible to quantify the impact of that measure, letting know from the start to all potential beneficiaries that the competent authorities

will make use of IT tools dedicated to the fight against fraud (such as EDES or ARACHNE) can have a deterrent effect on potential fraudsters.

In terms of reducing administrative burden and simplifying procedures, digitalisation of processes at the level of managing authorities reduces administrative burden for all stakeholders. It allows to gather data and documents on operations in a single IT tool that performs automated checks and cross-checks, that should have otherwise been performed by members of personnel (for example, thousands of invoices are uploaded into the IT tool that performs cross-checks between invoices of expenses declared in all projects and both ERDF and RFF funds in order to detect potential multiple declaration of same expenditures). Although, at EU level, the multiplicity of databases to consult in order to get a full picture (ARACHNE, EDES, Transparency System) sometimes constitutes an obstacle to reducing the administrative burden in the fight against fraud.

In terms of detection and administrative burden related to the use of ARACHNE : Since Wallonia started using ARACHNE (mid 2018) for ERDF, 432 risk (related to 25 different risks indicators) have been analysed. Following these analysis only one case led up to the uncovering of an irregularity that could have been a suspected fraud. It was however quickly established, in the course of the analysis, that there was no intention on the part of the beneficiary and the irregularity was consequently not qualified as suspected fraud and not communicated to OLAF (under the threshold of 10.000€ EU).

3.2.4. Strengthen fraud risk analysis

Q.1 Have you implemented the recommendation?

☒ YES, fully *ERDF and RRF Wallonia, ERDF Flanders, Department of Agriculture and Fisheries*

If you implemented fully the recommendation, can you please describe how you have done it? Can you share any specific findings? Please make a distinction between revenue and expenditure areas.

ERDF and RRF Wallonia : Wallonia is making use of informations and tools provided by the Commission in the area of fight against fraud.

Indeed, members of the personnel of the Managing authority take part in workshops and seminars provided by the Commission on the subject matter and meetings of working groups such as COCOLAF's working groups.

The knowledge basis acquired in shared management regarding fraud, corruption and conflict of interests is used and transposed, where possible, to RFF as the body in charge of PIF with regards to RFF is the same as for ERDF.

Wallonia feeds the ARACHNE tool with data from both ERDF program and RRF on a quarterly basis and communicates irregularities to OLAF for both funds, through IMS.

As foreseen in the Financial Regulation recast, Wallonia will make use of the EDES database in share management (ERDF), as well as for RRF.

Information is exchanged between relevant stakeholders implementing, controlling and auditing (at Wallonia's level) ERDF and RRF funds, through multiple channels (workings groups, monitoring committees, managing authority's website, ...) and all relevant data on expenditures, public procurement, detected irregularities and controls are accessible for these stakeholders, through specific and secured access, in the Managing authority's IT system.

ERDF Flanders:

In het kader van de Structuurfondsen legt de Algemene Verordening proportionele fraudebestrijdingsmaatregelen op. Bij de uitvoering van het EFRO-programma worden deze fraudemaatregelen beoordeeld door de Auditautoriteit. Het EFRO Vlaanderen programma behaalt hier een score 1 'het systeem werkt'.

Department of Agriculture and Fisheries:

Reeds langer wordt een proactieve aanpak aangehouden binnen het Departement Landbouw en Visserij. Specifiek in de context van de nieuwe programmaperiode die inging op 1/01/2023 wordt het risicobeheer verscherpt en herbekeken om een grotere focus te leggen op frauderisico's, waarbij alle subsidiemaatregelen en processen bekeken zullen worden om frauderisico's in kaart te brengen.

3.3. Bulgaria (BG)

3.3.1. Correct Transposition of the PIF Directive

Q.1. Has the Commission initiated infringement procedures against you for the incorrect transposition of the PIF Directive?

☒ NO

3.3.2. Participation in the EPPO

Q.1. Are you already participating in the EPPO?

☒ YES

The Prosecutor's office of the Republic of Bulgaria, according to its functions and competence, works in close interaction with all national law enforcement officials. By order of the General Prosecutor in 2021, in parallel with the start of the work of the EPPO, Department 08 "Crimes against the EU's financial interests and interaction with the European Public Prosecutor's Office" within the Supreme Cassation Prosecutor's Office was established in order to organize and ensure the interaction between the Prosecutor's Office of the Republic of Bulgaria and the European Public Prosecutor's Office, as well as optimizing the work of the Bulgarian prosecutors on files and pre-trial proceedings for crimes against the financial interests of the EU.

The fore-mentioned department, during the short period of its work by now, became contact point between PORB and OLAF, managed to achieve very high results in various directions of countering the crimes associated with European funds, as well as in increasing the efficiency in cooperation with all national and international partners in the field. The indisputable professional experience and capacity of the magistrates in this specialized national unit strengthened the authority of the Prosecutor's Office in interaction with the EPPO. Its representatives actively participate in all international events and forums in that area, participate as speakers/lecturers, not only by invitation of various institutions and organizations, but also initiate training modules for magistrates around the country, support the activities of working groups on amendments of the national legislation and transposition of European legislation, etc. All strategic analysis and targeted reports from the Commission, OLAF, EPPO, etc. are received, analyzed, taken into account and practically implemented according to the competences of the Prosecutor's Office.

3.3.3. Digitilising the fight against fraud

Q.1. Are you using any of the following IT systems in your fight against fraud?

☒ ARACHNE

☒ All EU funds and programmes (Cohesion, Rural Development, Recovery and Resilience Facility)

☒ IMS (do not select if IMS is used only for reporting irregularities and fraud, as this is a legal obligation. Select if irregularities and fraud reported via IMS are used to perform risk analysis or other anti-fraud related activities)

☒ National dedicated anti-fraud IT tools

Q.2. Has any interoperability been developed between EU IT tools and national IT tools?

☒ YES

Q.3. If yes, with which tool?

☒ ARACHNE

Q.4. To what end?

☒ Data enrichment

Q.5. How is digitalisation influencing the fight against fraud?

☒ Increasing prevention

☒ Increasing detection

☒ Reducing/simplifying administrative procedures

Q.6. For any impact selected, can you provide any quantification?

UMIS2020 is entirely web-based. The system is also designed to operate on mobile devices. The digitalisation of UMIS processes is our main tool for combating fraud. UMIS2020 is linked to several national systems, such as RegiX, Monitorstat and SAP. Given that each UMIS process is carried out in an electronic environment, we are able to collect lots of data in a structured form, which are then further processed and analysed. Alongside the internal system with its double funding functionalities and the system's e-service modules, the public module increases transparency as the public can monitor the entire grant award, implementation and reporting process through it, which increases the possibility of identifying and assessing projects with a high risk of fraud and irregularities at an early stage.

3.3.4. Strengthen fraud risk analysis

Q.1 Have you implemented the recommendation?

☒ YES, fully

If you implemented fully the recommendation, can you please describe how you have done it? Can you share any specific findings? Please make a distinction between revenue and expenditure areas.

The ARACHNE tool is used to perform checks when implementing the main assessment and negotiation processes before signing contracts with applicants (to check the absence/existence of double funding and to verify the absence/existence of a conflict of interest); when monitoring and verifying expenditure (checking that payments are made to a company registered in an area on a list of countries with offshore jurisdictions); before payment is made, to make sure that the beneficiary does not present a high risk of bankruptcy and/or insolvency and that it is not blacklisted. when examining and checking reported expenditure under a contract concluded with a contractor.

The 'Central Coordination Unit' Directorate at the Administration of the Council of Ministers has increased the number of users for the ongoing use of ARACHNE in the management of funds from ESIF/the Recovery and Resilience Plan as a tool for preventing irregularities and combating fraud. Increasing the number of users enables projects with a high risk of fraud, conflicts of interest and irregularities to be identified and assessed at the earliest possible stage.

When carrying out the fraud risk assessment, the competent authorities in Bulgaria also take into account the European Commission's Note Ref. Ares (2021) 3171797 – 12/05/2021 on the need to update fraud risk assessments and adapt anti-fraud measures.

The 'National Fund' Directorate, which performs the functions of the Certifying Authority and the Accounting Authority, falls under the Ministry of Finance.

Within the framework of its control functions as Certifying Authority, the National Fund Directorate is empowered to carry out checks where necessary and use the information contained in the European Commission's system for measuring the risk of fraud and irregularities (ARACHNE). In addition, when carrying out checks on compliance with the procedures and control activities of the managing authorities, the Certifying Authority's experts monitor the presence of 'red flags' referred to in documents issued by the European Anti-Fraud Office (OLAF) and the European Commission indicating fraud under the ERDF, ESF and CF and listed in detail in the checklists for the inspection of accounting documentation or the procedure for selecting contractors.

In relation to the Recovery and Resilience Facility, the National Fund Directorate within the Ministry of Finance acts as a coordinating unit at national level. The management and control system of the Recovery and Resilience Plan (RRP) incorporates checks in the ARACHNE tool, covering ex-post controls of public procurement procedures and verification of reported financial and technical information in connection with the performance of on-the-spot checks. This is part of the fraud risk assessment carried out by the National Fund Directorate, as a result of which checks on the information contained in the ARACHNE tool and checks using fraud indicators – red flags – have been introduced as controls that should have an impact on the identified risks.

In the RRP management and control system, the actions to be carried out in connection with the verification of conflicts of interest/related parties (ARACHNE system, Commercial Register, etc.) and the verification of double funding, including in the Financial Transparency System, are in place.

The management and control system also contains the procedure for reporting fraud, corruption and conflicts of interest from internal and external sources.

In connection with the implementation of the National Recovery and Resilience Plan, the UMIS 2020 information system provides the possibility of entering and storing the data referred to in Article 22(2)(d) of Regulation (EU) 2021/241, which is the responsibility of the final recipients and which is checked by the management and control authorities of the NRRP. The system also has modules for reporting and following up reports and incidents relating to irregularities.

The Executive Agency 'Audit of EU Funds', as the body responsible for carrying out specific audit activities on European Union funds and programmes, fully implements the recommendation for enhanced fraud risk analysis. During the course of auditing work, checks are carried out to identify fraud indicators, cases are analysed and presented in the annual control reports for each programme/financial instrument, and the competent authorities are also notified. The purpose of this analysis is to verify the proper functioning of the managing authorities' management and control systems.

In accordance with the Commission's Guidelines on fraud risk assessment and effective and proportionate anti-fraud measures, which we apply (EGESIF_14-0021 – 0016/06/2014), the handbook 'The role of Member States' auditors in fraud prevention and Detection for EU Structural and Investment Funds: experience and practice in the Member States', the Information Note on Fraud Indicators in relation to the ERDF, ESF and CF (COCOF 09/0003/00 – 18/2/2009), OLAF's Guidelines for identifying conflicts of interests in public procurement procedures for structural actions and the results of the audit carried out in 2022, the Executive Agency has notified the European Prosecutor's Office and the authorities of the Prosecutor's Office of the Republic of Bulgaria of 3 cases where suspicions of fraud and suspicions of agreements between undertakings/concerted practices have arisen.

The Public Procurement Agency reviewed and analysed information and data in the field of public procurement from reports and other documents issued by the Commission, the European Anti-Fraud Office, the Ministry of the Interior's AFCOS Directorate, the State Financial Inspection Agency, the Court of Auditors, the Commission for the Protection of Competition, the Managing Authorities of operational programmes, the Executive Agency 'Audit of EU Funds', the World Bank, the

Organisation for Economic Co-operation and Development, etc. In addition, the weightings of the risk factors for the methodology for the random selection of control procedures (in force since 1.1.2022) and the control opinion models have been updated.

The Customs Agency strives to use data from all available sources, both European and national. All the risk criteria under the Implementing Decision laying down measures for the uniform application of customs controls by establishing common financial risk criteria and standards have also been implemented. The information received is analysed and risk profiles are introduced on that basis. Where suspicion arises that a risk may occur in other Member States, the information is transmitted through CRMS, AFIS mail or national systems.

In June 2022, an Interaction and Cooperation Agreement was concluded between the State Agency for National Security, the Ministry of Innovation and Growth and the Ministry of the Interior. The aim of the agreement is to enhance and facilitate the exchange of information as well as the use of data from different sources to ensure better analysis in identifying and addressing emerging fraud risks and trends in a timely manner. As a result, coordination and interaction took place in 2022 with the Ministry of the Interior's AFCOS Directorate and the Ministry of Innovation and Growth, on cases concerning the possible existence of organised criminal schemes for the unlawful diversion and absorption of funds from EU financial programmes for the 2014 – 2020 programming period.

3.4. Cyprus (CY)

3.4.1. Correct Transposition of the PIF Directive

Q.1. Has the Commission initiated infringement procedures against you for the incorrect transposition of the PIF Directive?

☒ YES

Q.2. For the Member States having replied yes. Have you taken remedial action to modify national legislation?

☒ YES, for all launched infringements

Q.3. For the Member States having replied yes. By when do you expect to complete the modification of national legislation to correctly transpose the PIF Directive?

The draft law has been subjected to legal scrutiny and will be submitted for adoption once the House of Representatives reconvenes after the presidential elections taking place on 5 and 12 February 2023.

3.4.2. Participation in the EPPO

Q.1. Are you already participating in the EPPO?

☒ YES

3.4.3. Digitilising the fight against fraud

Q.1. Are you using any of the following IT systems in your fight against fraud?

☒ ARACHNE

☒ Recovery and Resilience Facility

Q.2. Has any interoperability been developed between EU IT tools and national IT tools?

☒ NO

Q.5. How is digitalisation influencing the fight against fraud?

☒ Increasing detection

☒ Reducing/simplifying administrative procedures

Q.6. For any impact selected, can you provide any quantification?

3.4.4. Strengthen fraud risk analysis

Q.1 Have you implemented the recommendation?

☒ YES, fully

If you implemented fully the recommendation, can you please describe how you have done it? Can you share any specific findings? Please make a distinction between revenue and expenditure areas.

The following were implemented during 2022:

Targeted fraud risk assessment for the recovery and resilience plan (RPP). The Commission's fraud risk assessment tool was used for this exercise. The tool covered the likelihood and impact of specific and commonly identified fraud risks related in particular to basic procedures: selection of applicants, implementation and verification, milestones and targets, and certification and payments. There were five steps to the methodology: quantifying the likelihood and impact of a specific fraud risk (gross risk); assessing the effectiveness of existing controls in mitigating gross risk; evaluating gross risk taking into account the impact and effectiveness of current controls (residual risk); assessing the impact of planned additional controls on the gross (residual) risk; and defining the target risk.

ARACHNE was used to complement the fraud risk assessment process, promoting use of an approach based on risk detection and scoring. This approach can increase the effectiveness of project selection, verifications and checking, and can further strengthen identification, prevention and detection of fraud, especially in cases of corruption. ARACHNE is used for the RPP, to prevent double funding and conflict of interests. There are also plans for it to be used for the cohesion policy funds for programming period 2021-2027.

Establishment of the Independent Anti-Corruption Authority The Authority is the designated competent authority for coordinating the actions of public sector services, the wider public sector and the private sector to prevent and combat corruption at national level. The Authority's responsibilities are laid down in Article 7 of Law 19(I)/2022 on the establishment and operation of the Independent Anti-Corruption Authority.

Guidelines approved by the Council of Ministers have been issued on procedures to ensure compatibility with national and EU public procurement policy, and for prevention, detection and correction of fraud, corruption and conflict of interests in the context of the RPP.

Two Regulatory Administrative Acts have been amended, implementing the national anti-money laundering law (Law 188 (I)/2007), in order to allow all national and EU control bodies access to beneficial ownership databases. RAA 116/2022 and RAA 180/2022 grant access to the relevant beneficial ownership databases with the Treasury of the Republic of Cyprus, Directorate-General for Development, Internal Audit Service, Auditor General, European Commission, Court of Auditors, OLAF and EPPO having the same rights as the competent national anti-money laundering authorities.

In addition, the Cyprus Agricultural Payments Organisation has carried out a fraud risk analysis of the projects/measures that it funds. Procedures for using the ARACHNE Risk Scoring Tool have also been introduced.

For revenues, and especially in relation to the Customs and Excise Department, all information received from the Commission and other Member States through CRMS2 and the AFIS portal is processed and analysed. Appropriate measures are then taken, mainly in the form of risk profiling, and alerts are sent to frontline officers.

With regards to financial risks, the Customs and Excise Department has applied the common criteria for financial risk for combating fraud in the following areas: undervaluation, misclassification, anti-dumping, preferential origin, quotas, suspensions, customs procedure 4200/6300, as well as risks related to specific economic operators and the nature of the goods.

The Post Control and Audit Department takes into account the above, and risk information forms (RIF), OLAF and statistics from own resources etc, when planning post-control audits, especially in cases where there is a reasonable suspicion of undervaluation, wrong tariff classification and failure to apply EU regulations on anti-dumping measures.

3.5. Czechia (CZ)

3.5.1. Correct Transposition of the PIF Directive

Q.1. Has the Commission initiated infringement procedures against you for the incorrect transposition of the PIF Directive?

☒ NO

3.5.2. Participation in the EPPO

Q.1. Are you already participating in the EPPO?

☒ YES

3.5.3. Digitilising the fight against fraud

Q.1. Are you using any of the following IT systems in your fight against fraud?

☒ ARACHNE

☒ All EU funds and programmes (Cohesion, Rural Development, Recovery and Resilience Facility)

☒ Recovery and Resilience Facility – *access to ARACHNE ensured, but for controls and verification of applicants rather the CRIBIS database is used.*

☒ other (specify)

Register of beneficial owners (Ministry of Justice database)

CRIBIS (commercial database of commercial information)

DATLAB (sophisticated database of procurements)

Q.2. Has any interoperability been developed between EU IT tools and national IT tools?

☒ YES

Q.3. If yes, with which tool?

☒ ARACHNE

Q.4. To what end?

☒ Data enrichment

☒ Introduce new red flags/risk indicators

☒ Fine tune/refine red flags/risk indicators/risk scoring

Q.5. How is digitalisation influencing the fight against fraud?

☒ Increasing prevention

☒ Increasing detection

☒ Reducing/simplifying administrative procedures

Q.6. For any impact selected, can you provide any quantification?

Not available.

3.6. Germany (DE)

3.6.1. Correct Transposition of the PIF Directive

Q.1. Has the Commission initiated infringement procedures against you for the incorrect transposition of the PIF Directive?

☒ NO

3.6.2. Participation in the EPPO

Q.1. Are you already participating in the EPPO?

☒ YES

3.6.3. Digitilising the fight against fraud

Q.1. Are you using any of the following IT systems in your fight against fraud?

In general, we would like to refer to the ongoing negotiations on the revision of the EU Financial Regulation. In this context, Germany has already sent the European Commission detailed questions on the proposed use of a data analysis and risk assessment tool (based on ARACHNE) and the Early Detection and Exclusion System (EDES).

We would also refer to Germany's replies to the Commission's 2022 ARACHNE user survey. The replies reflect the feedback received from all bodies responsible for managing and overseeing EU funds in Germany.

The issues and reservations raised now need to be clarified in detail during the negotiations.

No - Rhineland-Palatinate ERDF managing authorities

☒ EDES Mecklenburg-Western Pomerania ERDF managing authority

☒ IMS (do not select if IMS is used only for reporting irregularities and fraud, as this is a legal obligation. Select if irregularities and fraud reported via IMS are used to perform risk analysis or other anti-fraud related activities) *North Rhine-Westphalia and Mecklenburg-Western Pomerania ERDF managing authorities*

☒ other (specify) *Bavaria ERDF managing authority: There is an established procedure for detecting, reporting and monitoring the relevant data in general, and data on irregularities in particular. There is a database system for reporting and monitoring in the ERDF, IGJ Objective, Bavaria 2014-2020 (FIPS2014), which is also used for programme management.*

Q.2. Has any interoperability been developed between EU IT tools and national IT tools?

☒ NO *Brandenburg, Schleswig-Holstein, North Rhine-Westphalia, Bavaria, Saxony-Anhalt, and Mecklenburg-Western Pomerania ERDF managing authorities; Federal Ministry of Labour and Social Affairs*

Q.5. How is digitalisation influencing the fight against fraud?

☒ Increasing prevention *Bavaria ERDF managing authority*

☒ Increasing administrative burden *Mecklenburg-Western Pomerania ERDF managing authorities; Federal Ministry of Labour and Social Affairs*

☒ Reducing/simplifying administrative procedures *Brandenburg and Bavaria ERDF managing authorities*

Q.6. For any impact selected, can you provide any quantification?

Bavaria ERDF managing authority: Evaluation and follow-up are being facilitated. Federal Ministry of Labour and Social Affairs No

3.6.4. Strengthen fraud risk analysis

Q.1 Have you implemented the recommendation?

☒ YES, partly *Rhineland-Palatinate, North Rhine-Westphalia. and Mecklenburg-Vorpommern ERDF managing authorities, Federal Ministry of Labour and Social Affairs*

☒ NO *Brandenburg, Schleswig-Holstein, Bavaria, and Saxony-Anhalt ERDF managing authorities*

If you implemented partially the recommendation, could you please explain why you think it was a partial implementation and why a full implementation was not possible? Please make a distinction between revenue and expenditure areas.

In Rhineland-Palatinate (ERDF managing authority), the annual reports of the Regional Court of Auditors, the European Court of Auditors and the ERDF audit authority are being analysed and evaluated in terms of their relevance for the ERDF. If new risks are identified, they are integrated into the Rhineland-Palatinate fraud prevention tool. Because of staffing capacity we are unable to do more.

Mecklenburg-Western Pomerania ERDF managing authority: Data from various available sources are used and analysed and information is shared, including with law enforcement authorities. This ensures adequate prevention, detection and follow-up of fraud, while respecting the principle of proportionality. Not all available databases are being used.

Federal Ministry of Labour and Social Affairs As part of the support for the Federal Programme for the European Social Fund (ESF), all available resources are being used to fight fraud in order to ensure exchanges between the relevant stakeholders. This includes, in particular, regular self-assessment of the managing authority's strategic approach to preventing and combating fraud and corruption. This self-assessment includes all available information on combating fraud (for example, also up-to-date PIF reports) and exchanges between the relevant stakeholders, for example, on current cases of fraud and suspected fraud involving the ESF and the main identified risk areas, in order to investigate and address emerging risks and fraud trends in a timely manner.

If you did not implement the recommendation, could you please explain why?

Bavaria ERDF managing authority: There is already an established procedure for detecting, reporting and monitoring the relevant data in general, and data on irregularities in particular. Checklists are developed (for example, on conflicts of interest) on an ongoing basis, meaning that improvements are implemented in a timely manner. Audit priorities are dealt with using specially developed checklists that include fraud-related questions. Data storage and data exchange must comply with data protection requirements.

Federal Ministry of Food and Agriculture on the questions under 2.3 and 2.4: The questions cannot be answered in the requested format. ARACHNE and EDES are not used for agriculture and fisheries. In these areas, fraud prevention takes the form of regular analysis of specific fraud risks. This, along with appropriate training measures, is suitably provided for in the fraud prevention procedures of the

Länder and the Federal Government. For this purpose, use is also made of IMS data and Commission recommendations (such as PIF reports).

3.7. Denmark (DK)

3.7.1. Correct Transposition of the PIF Directive

Q.1. Has the Commission initiated infringement procedures against you for the incorrect transposition of the PIF Directive?

☒ NO

3.7.2. Participation in the EPPO

Q.1. Are you already participating in the EPPO?

☒ NO

Q.2. For the Member States not participating yet. Are there plans to join the EPPO in the short-medium term?

☒ NO

3.7.3. Digitilising the fight against fraud

Q.1. Are you using any of the following IT systems in your fight against fraud?

☒ IMS (do not select if IMS is used only for reporting irregularities and fraud, as this is a legal obligation. Select if irregularities and fraud reported via IMS are used to perform risk analysis or other anti-fraud related activities)

☒ other (specify) (*For cohesion: Project reporting data is linked with data from the business register and the income register*)

☒ National dedicated anti-fraud IT tools

Q.2. Has any interoperability been developed between EU IT tools and national IT tools?

☒ NO

Q.5. How is digitalisation influencing the fight against fraud?

☒ Increasing prevention

☒ Increasing detection

☒ Increasing administrative burden

Q.6. For any impact selected, can you provide any quantification?

3.7.4. Strengthen fraud risk analysis

Q.1 Have you implemented the recommendation?

☒ YES, partly

If you implemented partially the recommendation, could you please explain why you think it was a partial implementation and why a full implementation was not possible? Please make a distinction between revenue and expenditure areas.

For customs (revenue), the Danish Customs Agency uses data from all available sources, analyses and exchanges information including with Commission, and acts on specific analyses and reports. The Customs Agency does not necessarily act on all analyses and reports.

For agriculture (expenditure), the Danish Agricultural Agency has had a sectoral approach and has developed the use of national databases. From 2023, the efforts will be strengthened as a statutory risk assessment will be part of the accreditation conditions for authorities disbursing funds under the Common Agricultural Policy.

For cohesion (expenditure), the Danish Business Authority conducts data driven controls based on internal data linked with data from the business register and the income register. On the basis on the linked data, a risk assessment is carried out, but the data is not linked with other databases as in ARACHNE. The Danish Business Authority currently investigates the possibilities for supplementing the existing controls with ARACHNE.

For fisheries (expenditure), IMS is used to report irregularities to the Commission. Suspicion of fraud is reported directly to the appropriate authorities.

3.8. Estonia (EE)

3.8.1. Correct Transposition of the PIF Directive

Q.1. Has the Commission initiated infringement procedures against you for the incorrect transposition of the PIF Directive?

☒ YES

Q.2. For the Member States having replied yes. Have you taken remedial action to modify national legislation?

☒ NO

3.8.2. Participation in the EPPO

Q.1. Are you already participating in the EPPO?

☒ YES

3.8.3. Digitilising the fight against fraud

Q.1. Are you using any of the following IT systems in your fight against fraud?

☒ ARACHNE

☒ Cohesion (not all programmes)

☒ Rural Development

☒ other (specify) - *Estonian Tax and Customs Board is using different AFIS applications.*

☒ National dedicated anti-fraud IT tools – *We use national information systems for the implementation of support and these systems are connected to several national registers (Commercial Register, Public Procurement Register etc)*

Q.2. Has any interoperability been developed between EU IT tools and national IT tools?

☒ NO

Q.5. How is digitalisation influencing the fight against fraud?

☒ Increasing prevention

☒ Increasing detection

☒ Reducing/simplifying administrative procedures

3.8.4. Strengthen fraud risk analysis

Q.1 Have you implemented the recommendation?

☒ YES, fully (*REVENUE*)

☒ YES, partly (*EXPENDITURE*)

If you implemented fully the recommendation, can you please describe how you have done it? Can you share any specific findings? Please make a distinction between revenue and expenditure areas.

Estonian Tax and Customs Board is constantly and proactively using all available sources and data to better protect the EU's financial interests. The data is being shared with all relevant law

enforcement authorities including the Commission. One of the measures indicated in PIF questionnaire 2022 was:

To better protect the EU's financial interests, the Estonian Customs has created an IT tool, which automatically checks the declared prices against prices provided by the EU's database Theseus. This new approach has allowed Customs to extrapolate the use of Theseus to the broader scope of commodities, not being limited only by textiles or footwear. The new tool detects and identifies customs declarations with a risk of undervaluation, which need to be checked

If you implemented partially the recommendation, could you please explain why you think it was a partial implementation and why a full implementation was not possible? Please make a distinction between revenue and expenditure areas.

Estonian Managing Authority for ESIF programs has started again with the analysis of ARACHNE deployment. In 2022 we did the analysis of the data fields and the first testing. In 2023, the goal is to decide to what extent we will use ARACHNE and carry out the necessary training.

In addition, they have developed risk-based controls for the implementation of the period 2021-2027 and set the obligation to carry out a risk assessment (including fraud risks) already at the stage of developing support measures

Estonian Agricultural Register and Information Board uses ARACHNE as an additional source for a risk assessment.

3.9. Spain (ES)

3.9.1. Correct Transposition of the PIF Directive

Q.1. Has the Commission initiated infringement procedures against you for the incorrect transposition of the PIF Directive?

☒ YES

Q.2. For the Member States having replied yes. Have you taken remedial action to modify national legislation?

☒ YES, but not for all launched infringements

Q.3. For the Member States having replied yes. By when do you expect to complete the modification of national legislation to correctly transpose the PIF Directive?

By Letter of Formal Notice of 2 December 2021 (INFR 2021/2235) the European Commission notified the Kingdom of Spain of the non-compliance of Spanish legislation with Directive (EU) 2017/1371 (Directive on the fight against fraud to the Union's financial interests by means of criminal law) for failure to transpose correctly into national law:

- Article 4(2)(a) of the Directive*
- Article 4(2)(b) of the Directive*
- Article 7(1) in conjunction with Article 3(2)(a) and (b) of the Directive; and*
- Article 7(3) in conjunction with Article 4(2)(b) of the Directive.*

By means of a report and annex of case law from the Technical Secretary General of the Ministry of Justice, dated 24 January 2022, a response to this letter was given with an assessment of each and every one of the articles allegedly not transposed correctly, justifying their transposition.

Since the date of the report, no response has been received from the European Commission

3.9.2. Participation in the EPPO

Q.1. Are you already participating in the EPPO?

☒ YES

☐ NO

3.9.3. Digitilising the fight against fraud

Q.1. Are you using any of the following IT systems in your fight against fraud?

- ☒ ARACHNE
- ☒ Cohesion (not all programmes)
- ☒ other (specify) *National Grants Database, Public Sector Procurement Platform, Commercial Register, E-informa, Axesor, Infocif.*
- ☒ National dedicated anti-fraud IT tools

Q.2. Has any interoperability been developed between EU IT tools and national IT tools?

☒ YES

Q.3. If yes, with which tool?

☒ other (specify) *SFC (System for Fund Management in the European Union)*

As a general rule, interoperability between EU IT tools and national IT tools has not been developed.

However, according to the reply provided by the managing authority of the Asylum, Migration and Integration Fund (AMIF), they are working on the interoperability between the AMIF fund management application in Spain and the SFC application in order to carry out a more efficient and agile reporting of the management of the programme.

Q.4. To what end?

☒ Other (specify) *Management of the AMIF National Programme*

Q.5. How is digitalisation influencing the fight against fraud?

- ☒ Increasing prevention
- ☒ Increasing detection
- ☒ Increasing administrative burden
- ☒ Reducing/simplifying administrative procedures

The digitisation of the fight against fraud mostly involves an increase in fraud prevention and detection, as well as a simplification of administrative procedures. In some cases, it has also been suggested that it increases the administrative burden.

Q.6. For any impact selected, can you provide any quantification?

According to the information received, it is not possible to provide any quantification.

3.9.4. Strengthen fraud risk analysis

Q.1 Have you implemented the recommendation?

- ☒ YES, fully
- ☒ YES, partly

If you implemented fully the recommendation, can you please describe how you have done it? Can you share any specific findings? Please make a distinction between revenue and expenditure areas.

If you implemented partially the recommendation, could you please explain why you think it was a partial implementation and why a full implementation was not possible? Please make a distinction between revenue and expenditure areas.

Once the different authorities involved have been consulted, the conclusion that can be drawn based on their responses is that the measure has been partially implemented on the expenditure side and fully implemented on the revenue side.

Some of the reasons for this partial implementation on the expenditure side are as follows: they are in the process of implementing national tools, or they plan to implement them later depending on the technical requirements and/or necessary resources, or they do not consider that the recommendation has been fully implemented as they do not use the IT tools recommended by the Commission.

In some cases, it has been indicated that it is difficult to obtain all the information on the cases given the distribution of competences between the different bodies involved. In general, the good collaboration of all the authorities managing European funds with AFCOS and OLAF in the collection and forwarding of the information requested in their investigations is highlighted.

We highlight below some of the responses to the recommendations adopted.

In the area of expenditure:

In the case of European Territorial Cooperation, the database is common for all cooperation programmes in which Spain participates, which allows taking into account the common information on risks and warning flags of the different programmes.

The European Social Fund (ESF) authorities report that work is underway to strengthen anti-fraud mechanisms in the management of this fund, considering that the development and implementation of the National Anti-Fraud Strategy will serve to improve its procedures.

Anti-Fraud Action Plans have been developed for the management of funds from the Recovery and Resilience Mechanism, and Anti-Fraud Units or Committees have been set up.

On the revenue side, the implementation of the recommendation has been full. The State Tax Administration Agency, which is responsible for the management of the state tax and customs system, has a Consolidated Database that allows the implementation of risk analysis systems based on Data Analytics. It also applies a risk analysis system in which it uses all available sources of information, whether internal databases, open source information, complaints received or data from OLAF or other Community bodies.

In particular, the Tax Agency maintains a very active position in the EUROFISC¹⁵ group to combat organised intra-Community VAT fraud, and maintains a very fluid relationship with the other Member States for the exchange of sensitive information, both on specific cases of non-compliance and on evasion procedures or techniques.

The exchange of information with law enforcement authorities is possible, although it is restricted to the legal framework of protecting the confidentiality and secrecy of information of a tax nature.

¹⁵ EUROFISC is a network of VAT antifraud experts, established and funded by the EU Fiscalis programme.

3.10. Finland (FI)

3.10.1. Correct Transposition of the PIF Directive

Q.1. Has the Commission initiated infringement procedures against you for the incorrect transposition of the PIF Directive?

☒ YES

Q.2. For the Member States having replied yes. Have you taken remedial action to modify national legislation?

☒ NO

Q.3. For the Member States having replied yes. By when do you expect to complete the modification of national legislation to correctly transpose the PIF Directive?

The Finnish Government has replied to the Commission's letter of formal notice in case INFR(2021)2234. We consider that the Directive has been adequately and correctly implemented in Finland.

3.10.2. Participation in the EPPO

Q.1. Are you already participating in the EPPO?

☒ YES

3.10.3. Digitilising the fight against fraud

Q.1. Are you using any of the following IT systems in your fight against fraud?

☒ other (specify) *National programme information systems and business data (the Asiakastieto service)*

Q.2. Has any interoperability been developed between EU IT tools and national IT tools?

☒ NO

Q.5. How is digitalisation influencing the fight against fraud?

☒ Increasing prevention

☒ Increasing administrative burden

3.10.4. Strengthen fraud risk analysis

Q.1 Have you implemented the recommendation?

☒ YES, partly

If you implemented partially the recommendation, could you please explain why you think it was a partial implementation and why a full implementation was not possible? Please make a distinction between revenue and expenditure areas.

For revenue, Finnish Customs has developed and automated the processing of data from official sources (e.g. CRM2, AFIS/MAS) to detect risks. This will enable Customs to address the risks in a timely manner.

For expenditure, steps have been taken in the area of data analysis, in particular the implementation of the RRF. A joint government project portfolio and RRP system have been put in place to monitor aid granted under the RRF. Information on granting and paying aid, beneficial owners and DNSH assessments has been entered into the systems. The various aid authorities must enter up-to-date information in the systems every month. This information is also available to the RRP's control and inspection authorities. These systems will help meet the needs for data availability and coverage. Data quality is ensured by control and audit activities. Information on the findings of control and audit measures carried out by the aid authorities will also be recorded in the systems.

The option of using the Commission's data management and extraction tool (ARACHNE) has been explored as part of preparations for implementing the RRF. So far, no decision to introduce the tool has been taken for the RRF or for other EU programmes. The main problems with access to different Commission information systems and data tools relate to limited resources, i.e. increased administrative burden, and legislation, in particular as regards the transmission of personal data and data protection.

Other actions have also been taken at the paying agency responsible for agricultural funds, where anti-fraud activities have been reorganised. This means that information from different sources will be taken into account in the identification of fraud risks and in the design of anti-fraud measures to a greater extent than previously.

Preventive anti-fraud measures in the Home Affairs Funds are also implemented through training and guidance and risk-based control and audit activities.

3.11. France (FR)

3.11.1. Correct Transposition of the PIF Directive

Q.1. Has the Commission initiated infringement procedures against you for the incorrect transposition of the PIF Directive?

☒ NO

3.11.2. Participation in the EPPO

Q.1. Are you already participating in the EPPO?

☒ YES

3.11.3. Digitilising the fight against fraud

Q.1. Are you using any of the following IT systems in your fight against fraud?

☒ ARACHNE

☒ Cohesion (not all programmes)

☒ other (specify) *The managing authorities use various databases for management verifications (Manageo, Fiben, Societe.com, Infogreffe, Diane, etc.).*

☒ National dedicated anti-fraud IT tools

Q.2. Has any interoperability been developed between EU IT tools and national IT tools?

Automated data exchange between information systems has not been implemented. At present, in order to use ARACHNE and IMS, data has to be exported from the Synergie information system (the tool for managing and monitoring European programmes in France) by means of a file. The ANCT [National Agency for Territorial Cohesion], which is responsible for Synergie, is investigating the possibility of automating data exchange between Synergie and the ARACHNE and IMS information systems.

Q.5. How is digitalisation influencing the fight against fraud?

☒ Increasing prevention

☒ Increasing administrative burden

Q.6. For any impact selected, can you provide any quantification?

While the ARACHNE system does enhance the prevention of fraud relating to EU funds, it also increases the administrative burden for staff responsible for management verifications. ARACHNE contains an array of information that makes it difficult to understand, with risk indicators that are difficult to interpret.

However, the authorities managing EU funds also use various databases which can be consulted instead of or as well as ARACHNE (Manageo, Fiben, Societe.com, Infogreffe, Diane, etc.). The consultation of digital tools or information systems for data on beneficiaries of EU funds is integrated into managing authorities' management verification procedures and anti-fraud measures.

3.11.4. Strengthen fraud risk analysis

Q.1 Have you implemented the recommendation?

☒ YES, fully

If you implemented fully the recommendation, can you please describe how you have done it? Can you share any specific findings? Please make a distinction between revenue and expenditure areas.

MICAF [the Inter-Ministerial Anti-Fraud Coordination Mission] has drawn up a new national strategy to combat fraud affecting the EU budget. The aim is to prevent fraud through better risk management, to detect fraud by strengthening data collection, sharing and processing, and to prosecute and punish fraud by improving administrative and judicial coordination.

In this context, the ANCT leads working groups involving all the managing authorities for EU funds, with the aim of consolidating and harmonising the existing arrangements for the prevention, detection and reporting of fraud.

The managing authorities for EU funds use various databases which can be consulted instead of or as well as ARACHNE with regard to fraud prevention. The managing authorities also exchange information relating to operational data in order to avoid any risk of double funding from EU funds.

Moreover, with regard to fraud prevention and identifying fraud risks, the information notes and practical guides drawn up by the Commission on fraud warning signs have been distributed to the authorities managing EU funds. The European Public Prosecutor's Office has attended a number of meetings organised by the ANCT with the managing, certification and audit authorities to explain its role in supporting managing authorities in the fight against fraud affecting EU funds and the practicalities of working and exchanging information with the Office. These meetings were attended by technicians and decision-makers from the managing authorities.

In this context, the MICAF had the opportunity to present its tasks and its procedure for cooperation between managing authorities and the European Public Prosecutor's Office.

Finally, the MICAF has opened up its training catalogue to all those involved in the management of EU funds in order to provide them with access to training delivered by anti-fraud professionals. The ANCT relays the information through its collaborative platform, and managing authority staff have already attended various training sessions.

3.12. Greece (GR)

3.12.1. Correct Transposition of the PIF Directive

Q.1. Has the Commission initiated infringement procedures against you for the incorrect transposition of the PIF Directive?

☒ YES

Q.2. For the Member States having replied yes. Have you taken remedial action to modify national legislation?

☒ YES

Q.3. For the Member States having replied yes. By when do you expect to complete the modification of national legislation to correctly transpose the PIF Directive?

3.12.2. Participation in the EPPO

Q.1. Are you already participating in the EPPO?

☒ YES

3.12.3. Digitilising the fight against fraud

Q.1. Are you using any of the following IT systems in your fight against fraud?

☒ ARACHNE

☒ Recovery and Resilience Facility

☒ other (specify) *RRF Management Information System*

Q.2. Has any interoperability been developed between EU IT tools and national IT tools?

☒ NO

3.12.4. Strengthen fraud risk analysis

Q.1 Have you implemented the recommendation?

☒ YES, fully

If you implemented fully the recommendation, can you please describe how you have done it? Can you share any specific findings? Please make a distinction between revenue and expenditure areas.

Division for Financial Control and Audit and Cooperative Affairs of the Ministry of Rural Development and Food:

The Division for Financial Control and Audit and Cooperative Affairs (Department for the Control of EAGF Expenditure), in application of Regulation (EU) No 1306/2013 of the European Parliament and of the Council, carries out ex post controls on beneficiaries or debtors directly or indirectly related to the financing system under the European Agricultural Guarantee Fund (EAGF) or their representatives.

The aim of these ex post controls is to scrutinise the commercial documents of those entities which are beneficiaries or debtors and which relate directly or indirectly to the financing system under the

EAGF or their representatives ('undertakings'), in order to ascertain whether EAGF transactions forming part of the financing system have actually been carried out and whether they have been executed correctly, based on the risk presented by the beneficiary, the risk of the measure under scrutiny, by means of specific control procedures and evidence, and the recovery of amounts wrongly paid.

The directorate carries out systematic scrutiny of the commercial documents of undertakings, taking account of the nature of the transactions to be scrutinised. The selection of undertakings for the annual control plan gives the best possible assurance of the effectiveness of the measures for preventing and detecting irregularities

A risk analysis methodology is therefore used, not only during the selection of undertakings for the control plan but also during the actual scrutiny of these undertakings. The risk analysis includes specific risks and risk values, all of the data relating to the scrutiny, and information from the Commission, in order to address any emerging risks

The selection takes into account, inter alia, the financial importance of the undertakings in that system and of other risk factors.

The accuracy of primary data under scrutiny is verified by a number of cross-checks, including, where necessary, the commercial documents of third parties, appropriate to the degree of risk presented, such as:

- a) comparisons with the commercial documents of suppliers, customers, carriers or other third parties;*
- b) physical checks, where appropriate, on the quantity and nature of stocks;*
- c) comparisons with the records of financial flows preceding or following the EAGF transactions carried out within the financing system, and*
- d) checks, in relation to bookkeeping or records of financial movements showing, at the time of the scrutiny, that the documents held by the paying agency by way of justification for the payment of aid to the beneficiary are accurate.*

Recovery and Resilience Facility Agency:

In accordance with Decision 129397/13-09-2022 of the Governor of the Recovery and Resilience Facility Agency (online publication No ΨΜ5KH-AΞΘ), a fraud risk assessment team was set up and an officer at the agency was designated as responsible for fraud issues. Furthermore, by Decision 135896/21-09-2022 of the Governor, the Recovery and Resilience Facility Agency's risk assessment methodology for the ex ante check for conflicts of interest when awarding public contracts was approved, in order to prevent, and enforce measures to assess and address, risks that may affect the smooth implementation and achievement of the Recovery and Resilience Facility Agency's objectives.

Directorate-General for Customs and Excise of the Independent Authority for Public Revenue:

Customs controls are carried out based on risk analysis in accordance with Article 46 of the Union Customs Code. The analysis makes use of all available information, particularly information from OLAF's mutual assistance messages and RIFs, and creates the corresponding risk profiles. Feedback on the measures taken is systematic and the monitoring of fraud risks and trends is ongoing.

3.13. Croatia (HR)

3.13.1. Correct Transposition of the PIF Directive

Q.1. Has the Commission initiated infringement procedures against you for the incorrect transposition of the PIF Directive?

☒ YES

Q.2. For the Member States having replied yes. Have you taken remedial action to modify national legislation?

☒ NO

Contribution of the Ministry of Justice and Public Administration:

The Republic of Croatia submitted in January 2022 a reply to the European Commission in relation to the letter of official notification on the transposition of the PIF Directive into the national criminal legislation.

3.13.2. Participation in the EPPO

Q.1. Are you already participating in the EPPO?

☒ YES

3.13.3. Digitilising the fight against fraud

Q.1. Are you using any of the following IT systems in your fight against fraud?

☒ ARACHNE

☒ Cohesion (all programmes) (*Ministry of Regional Development and EU Funds, Agency for the Audit of European Union Programmes Implementation System*)

☒ Rural Development (*Ministry of Agriculture*)

☒ Recovery and Resilience Facility (*Agency for the Audit of European Union Programmes Implementation System*)

☒ IMS (do not select if IMS is used only for reporting irregularities and fraud, as this is a legal obligation. Select if irregularities and fraud reported via IMS are used to perform risk analysis or other anti-fraud related activities) (*Ministry of Agriculture*)

☒ National dedicated anti-fraud IT tools (*e.g. web data bases, Companies register, Poslovna.hr, etc. - Agency for the Audit of European Union Programmes Implementation System*)

Q.2. Has any interoperability been developed between EU IT tools and national IT tools?

☒ NO

Q.5. How is digitalisation influencing the fight against fraud?

☒ Increasing prevention (*Agency for the Audit of European Union Programmes Implementation System, Ministry of Agriculture*)

☒ Increasing detection (*Agency for the Audit of European Union Programmes Implementation System*)

☒ Reducing/simplifying administrative procedures (*Agency for the Audit of European Union Programmes Implementation System, Ministry of Agriculture*)

☒ Other (specify) (*Ministry of Regional Development and EU Funds*)

Contribution of the Ministry of Regional Development and EU Funds:

ARACHNE - The ARACHNE Risk Scoring Tool will alert the Managing Authority in identifying projects, contracts, contractors and beneficiaries with highest risk, and help to focus on their administrative capacity for verifications. Where the analysis by the Managing Authority leads to recurring risks being identified, the management and control systems should be reinforced in order to prevent the risk from occurring in future.

ARACHNE is used while evaluating projects applying for funds in European structural and investment fund: Operational Program Competitiveness and Cohesion 2014-2020. It is also planned to use it for evaluation of projects in the Multiannual Financial Framework 2021-2027: Competitiveness and Cohesion Program 2021-2027.

In the feedback from the national implementing and intermediary bodies that use the relevant tool ARACHNE in their work within Operational Program Competitiveness and Cohesion 2014-2020, we received interesting observations and suggestions for improvement. Some of them are listed below:

- *The data in ARACHNE should be updated more frequently. The tool should have more financial data to make a quality risk assessment and search filter should include "search by a unique identifier number" dependant on the state. They use the tool in evaluation of project applications as well as in verification of procurement procedures (ex-post verification) and to detect conflict of interest. However, its usefulness might be improved. The data is often outdated and incomplete; it takes a lot of time to use it without significant impact (no conflicts of interest that we are aware of was detected through ARACHNE). There are much more effective means of detecting real and serious conflicts of interest and they are not at the disposal of Managing Authority or delegated intermediate bodies. For example tracking payments between legal entities and natural persons, gathering correspondence, conducting investigations, and these are not and cannot be at our disposal having in mind we are not formal investigative or prosecution bodies or financial authorities. Even if we were to file reports about suspicious behaviour or possible conflicts of interest, there would have to be a reasonable doubt before that, and with our current competences, we cannot achieve that goal. Therefore, use of ARACHNE is not useful.*
- *ARACHNE, as it is stipulated by the Managing Authority in the Common National Rules, does not serve for risk scoring, it serves to detect possible conflict of interest. To be used as a risk scoring tool, it should be used by the bodies in charge of programming and drafting/publishing calls for proposals, sectoral bodies, not bodies in charge of verification of funds and overseeing project implementation.*
- *The data should be valid, recent and complete.*
- *By clear communication from the European Commission level about the purpose of the system, perhaps focusing on lesser number of areas covered by the system, but make it more efficient.*
- *The three-month regular updates on companies publicly available information provided by ARACHNE is a too long period for the purpose of effective risk analysis. We have national and private databases with paid membership that provide this data on a more regular basis.*
- *Considering that we primarily use ARACHNE to check conflicts of interest, we believe that more data on companies and persons should be transferred to ARACHNE from court registers, trade registers and other relevant registers of member countries in order to have more data and a more accurate checks (official relevant internal pages: Poslovna.hr, InfoBiz, Tax Administration, official court registry, beneficial ownership register, trade register).*

ARACHNE tool can be used to strengthen the capacity to detect, report and follow-up on irregularities. Further improvements of IT systems and staff's competences are needed.

Q.6. For any impact selected, can you provide any quantification?

Contribution of the Ministry of Agriculture:

The usage of IT systems for the purpose of internal controls reduces administrative burden especially when compared with results it can provide.

At this moment, we do not have data to quantify the effect of digitization on increased prevention of possible fraud and/or reduction of administrative burden when conducting controls.

Contribution of the Agency for the Audit of European Union Programmes Implementation System (Audit Authority):

Digitalisation is indeed accelerating and facilitating the whole process. In other words, the information is much more accessible, transparent and reachable. Its processing is also easier and more available. During audit tests and checks, auditors check how the bodies in the management and control systems undertake anti-fraud measures and how they in practice protect the financial interests of the EU, also by using respective IT tool. The procedures at national level for all EU funds utilised and managed envisage and define roles, responsibilities and functions in respect of protection of EU funds as well. Tools, methods, instructions, guidelines are provided for all EU funds.

What should be improved is making the use of these tools and methods faster and getting/using all benefits that the tools provide. For this purpose, trainings should be organised at levels of all bodies (within management and control systems, at the level of coordinating bodies, audit authority, etc.) to train the staff on using all tools in the most effective, useful and productive way. One of the crucial things is then to upload and update the information in the digitalised systems as databases and to provide up-to-date, reliable and verifiable source of information.

3.13.4. Strengthen fraud risk analysis

Q.1 Have you implemented the recommendation?

☒ YES, fully (*Ministry of Regional Development and EU Funds, Agency for the Audit of European Union Programmes Implementation System*)

☒ YES, partly (*Ministry of Agriculture*)

If you implemented fully the recommendation, can you please describe how you have done it? Can you share any specific findings? Please make a distinction between revenue and expenditure areas.

If you implemented partially the recommendation, could you please explain why you think it was a partial implementation and why a full implementation was not possible? Please make a distinction between revenue and expenditure areas.

Contribution of the Ministry of Regional Development and EU Funds:

In relation to the risk assessment in the Operational Program Competitiveness and Cohesion 2014-2020, all bodies in the system of management and control of ESI funds since the beginning of the implementation of the Program, regardless of whether a risk assessment has been carried out, implement fundamental measures to combat fraud as follows:

conducting appropriate trainings and educations for employees of bodies in the system and the obligation to spread the acquired knowledge and obtained materials within the body (by delivering

them to the internal organizational unit/person in charge of education issues/coordinator for training, who then forwards them to all other organizational units);

at workshops intended for users: informing users about the measures taken for the purpose of prevention, detection and ways of dealing with established fraud (special attention is paid to (public) procurement issues) and the consequences to which they are exposed in cases of fraudulent behaviour (criminal prosecution, obligation to return 100% of the funds received), while referring the user to a website and/or e-mail address where suspected fraud can be reported anonymously;

regular monitoring of the OLAF website and the publication of reports by the European Court of Auditors dealing with the subject of irregularities, fraud and corruption to the detriment of the EU budget is the responsibility of the Risk Management Person or the Coordinator for Anti-Fraud Measures, who at least twice a year delivers a summary of the relevant data and documents published on the specified page to the heads of organizational units within their body and other risk owners (strategies, reports, presentations, brochures, a description of the cases that have been dealt with, etc.), who then pass them on to officials within their services/departments;

in relation to public procurement procedures, it is the duty of the Risk Management Person or the Coordinator for Anti-Fraud Measures to encourage project managers to regularly monitor the Electronic Public Procurement Bulletin (EOJN), the websites of the State Commission for the Control of Public Procurement Procedures (DKOM) and other national relevant websites and search engines (such as www.strukturnifondovi.hr, www.poslovna.hr, <https://sudreg.pravosudje.hr>) and to use the ARACHNE tool; verify the user and/or the person authorized to represent the user through the ARACHNE system and through some of the available Internet browsers regarding the prevention of conflicts of interest.

After performing the risk assessment, if necessary, additional, appropriate measures are taken, which are defined in relation to the identified risks and their reach.

Through cooperation with the Service for Coordination of the Anti-Fraud Coordination System related to EU funds (AFCOS-Service) as an organizational unit of the Ministry of Finance of the Republic of Croatia which performs a coordinating role within the AFCOS-system and acts as the main contact point for the European Anti-Fraud Office (OLAF) the task of protecting the financial interests of the EU is enhanced.

Cooperation with judicial bodies and services of the European Commission is stipulated in the Common National Rules for the Operational Program Competitiveness and Cohesion 2014-2020. In cases where it is considered that a specific, established irregularity contains elements of a criminal offense or fraud, the intermediary body that made the Decision on irregularity, along with all relevant documentation, shall without delay submit it to the State Attorney's Office of the Republic of Croatia. On the day of becoming aware of the fact that the committed criminal offense has been established by a final court decision, the intermediary body draws up an official note on the aforementioned, which it records in the Register of Irregularities and stores it in the eFondovi system and/or ESIF MIS. Also, the intermediary body informs the Ministry of Finance about suspected fraud through the IMS system in case of established irregularities with suspected fraud, if there is evidence based on which further payments within the project would not be justified and reasonable in the context of the obligation to protect national financial interests and financial interests of the European Union, and in this context a criminal complaint has been filed or is intended to be filed with the State Attorney's Office of the Republic of Croatia.

Contribution of the Ministry of Agriculture:

Data sources and data types which Croatian authorities already use or expect to collect and use (in period of new CAP 2023.—2027.) to monitor implementation (or evaluation) of agricultural policy are, among others, as follows:

- *administrative IT resources (reports, etc.)*
- *publicly available information (i.e. internet sites and other public data)*
- *remote sensors*
- *Earth observation technology and space/satellite technology (satellite data collection, program Copernicus Sentinel)*
- *mobile applications*
- *Geospatial data (data with geographical or location component-GSA).*

For the purpose of monitoring and evaluating measures within Common Agricultural policy, the analytical processing of large amounts of data is continuously used.

Croatian Paying Agency, also collects and processes data relevant to analyses of agricultural policy which are obtained through the system of IACS (Integrated Administrative and control system) as it is stipulated by relevant EU legislation.

Currently, the Croatian Paying Agency is in process of further developing and setting up of wider usage of Area Monitoring System (AMS) what includes the use of satellite data for the purpose of controls and analyses.

Beside this, ARACHNE system is used in Croatia as a basis for indication of the need to carry out additional controls in some doubtful projects.

In our understanding, it is crucial to improve and upgrade collecting of data so that they can be used, among other purposes, also for analyses related to fraudulent irregularities and fraud risks. Collected data and their quality are the basis for the quality risk analysis.

Additionally, Croatian authorities (Ministry of Agriculture and Croatian Paying Agency) continuously work on the quality of flow of information between organisational units dealing with controls and analyses.

National control system set up to implement for reforms and investments within the scope of Recovery and Resilience Facility also includes the use of ARACHNE. Ministry of Agriculture is responsible authority for the subcomponent C1.5. "Improving the use of natural resources and strengthening the supply chain" of National recovery and resilience plan and Ministry of Regional Development and EU Funds provides employees with access to the ARACHNE system and does the work of collecting and entering data into the ARACHNE system. This will strengthen capacity to detect, report and follow-up on irregularities, especially those on conflict of interest and will also serve as a basis for the risk analyses.

However, we consider this recommendation has been partially implemented as further improvements of Croatian Paying Agency's IT systems and upgrade of managing information on the level of Managing Authority and Croatian Paying Agency for the purpose of risk analyses are needed.

Contribution of the Agency for the Audit of European Union Programmes Implementation System (Audit Authority):

For example, the Audit Authority for the Recovery and Resilience Facility (RRF) in Croatia has issued a finding related to strengthening anti-fraud measures, with particular emphasis on performing of risk analyses. The auditees – all bodies encompassed by the audit, have prepared their risk analyses, based on the procedures outlining the methodology, the approach, providing templates, etc.

The Audit Authority is within their audits closely following the risk and irregularity management policies and processes. The Audit Authority is also highlighting that awareness should be continuously and regularly raised in the institutions falling under the management and control systems, with respect to fraud risk analyses; and trainings should be provided to all the staff dealing with EU funds/RRF.

The Audit Authority also provided inputs and contributed to the Questionnaire developed for the analysis of the system for combatting irregularities and fraud by the AFCOS Service. The analysis serves perfectly to evaluate the current state of play as regards the AFCOS network and system in Croatia. The Audit Authority expressed the viewpoints that staff in the management and control systems should be trained on all steps/processes in respect of prevention, detection, processing, reporting, follow-up of irregularities/fraud + applying of financial corrections; additionally, awareness should be raised on the bodies involved in the AFCOS network and their role in fraud management.

3.14. Hungary (HU)

3.14.1. Correct Transposition of the PIF Directive

Q.1. Has the Commission initiated infringement procedures against you for the incorrect transposition of the PIF Directive?

☒ YES

Q.2. For the Member States having replied yes. Have you taken remedial action to modify national legislation?

☒ NO

Q.3. For the Member States having replied yes. By when do you expect to complete the modification of national legislation to correctly transpose the PIF Directive?

Judit Varga, Minister for Justice, wrote to the Commission on 19 July 2022 setting out the relevant Hungarian law and practice and referring to the relevant international legal obligations and, for example, the GRECO findings. The Minister informed the Commission that the Hungarian Government considered the Hungarian legislation to be in line with the Directive.

3.14.2. Participation in the EPPO

Q.1. Are you already participating in the EPPO?

☒ NO

Q.2. For the Member States not participating yet. Are there plans to join the EPPO in the short-medium term?

☒ NO

3.14.3. Digitilising the fight against fraud

Q.1. Are you using any of the following IT systems in your fight against fraud?

☒ ARACHNE

☒ Cohesion (all programmes)

☒ Recovery and Resilience Facility

☒ EDES

Q.2. Has any interoperability been developed between EU IT tools and national IT tools?

☒ NO

Q.5. How is digitalisation influencing the fight against fraud?

☒ Increasing prevention

☒ Increasing detection

3.14.4. Strengthen fraud risk analysis

Q.1 Have you implemented the recommendation?

☒ YES, partly

If you implemented partially the recommendation, could you please explain why you think it was a partial implementation and why a full implementation was not possible? Please make a distinction between revenue and expenditure areas.

Revenue area

To support the uniform protection of the EU's financial interests, the Commission has adopted a Decision on Financial Risk Criteria (Implementing Decision C(2018) 3293 final establishing common financial risk criteria and standards, 'the FRC Decision') and Guidance on the implementation of the FRC Decision (TAXUD A3/057/2019).

The decision and the guidance will help to ensure a consistent approach to and consistent analysis and profiling (i.e. defining and flagging) of financial risks and uniform recording of abuses detected (with a two-digit FRC code clearly assigned to each financial risk and displayed next to the risk flag in the risk management system built into the process). The built-in risk management system developed by the National Tax and Customs Administration (NAV) enables real-time collection and evaluation of risk information and, where necessary, immediate intervention in the areas of both customs and tax.

The Commission regularly monitors the implementation of the Decision by means of a specific questionnaire and, on that basis, evaluates the related activities and makes recommendations to the Member States. FRC risks identified are shared between national customs authorities, including the NAV, and with the Commission.

The risks identified are managed according to their importance and are forwarded as a matter of priority to the competent specialists for further action, for example in the area of tax or criminal law.

It is also important to mention the integrated practice of the NAV, developed to protect the EU's financial interests, in which, following the customs procedure, our authority creates incentives for compliance for companies with mainly tax debts which show a low willingness to pay and are difficult to contact (after the release of customs goods, action may be taken by the authorities as long as the goods are available).

Expenditure area

FAIR, the information system for managing and recording Hungary's support from the operational programmes, is continually being developed, including building in fraud prevention functions. FAIR receives information from several domestic public databases, thus increasing the credibility of the data and reducing the administrative burden for beneficiaries. In addition, warnings drawing attention to potential risks have been built into the system.

The anti-fraud and anti-corruption strategy for European Union funds adopted by Government Decree No 1540/2022 of 15 November 2022 is also a significant step forward in the implementation of the recommendation. The strategy's action plan also proposes a number of further measures in line with the recommendation.

3.15. Ireland (IE)

3.15.1. Correct Transposition of the PIF Directive

Q.1. Has the Commission initiated infringement procedures against you for the incorrect transposition of the PIF Directive?

☒ NO

3.15.2. Participation in the EPPO

Q.1. Are you already participating in the EPPO?

☒ NO

Q.2. For the Member States not participating yet. Are there plans to join the EPPO in the short-medium term?

☒ NO

3.15.3. Digitilising the fight against fraud

Q.1. Are you using any of the following IT systems in your fight against fraud?

☒ IMS (do not select if IMS is used only for reporting irregularities and fraud, as this is a legal obligation. Select if irregularities and fraud reported via IMS are used to perform risk analysis or other anti-fraud related activities)

3.16. Italy (IT)

3.16.1. Correct Transposition of the PIF Directive

Q.1. Has the Commission initiated infringement procedures against you for the incorrect transposition of the PIF Directive?

☒ NO

3.16.2. Participation in the EPPO

Q.1. Are you already participating in the EPPO?

☒ YES

3.16.3. Digitilising the fight against fraud

Q.1. Are you using any of the following IT systems in your fight against fraud?

☒ ARACHNE

☒ All EU funds and programmes (Cohesion, Rural Development, Recovery and Resilience Facility)

☒ EDES

☒ IMS (do not select if IMS is used only for reporting irregularities and fraud, as this is a legal obligation. Select if irregularities and fraud reported via IMS are used to perform risk analysis or other anti-fraud related activities)

☒ National dedicated anti-fraud IT tools

Contribution by the General Inspectorate for Financial Relations of the State General Accounting Department – MEF

In 2022, the first trials started with the Integrated Anti-Fraud Platform PIAF, which interacts with and collects data from heterogeneous and certified external sources at national and European level. The objective of the platform is to consolidate and strengthen the fight against fraud and other illegal activities to the detriment of the EU budget through technical and operational support for national and transnational investigations.

The platform collects data from the following sources and databases:

- *Agenzia delle Entrate (Revenue Agency (Tax Register))*
- *Infocamere (official Chamber of Commerce site) (Chamber of Commerce Register)*
- *Court of Auditors (online consultation tool - GIUDICO; Irregularities and Fraud Information System – SIDIF)*
- *Ministry of Economic Affairs and Finance, General Inspectorate for Financial Relations with the European Union (MEF-IGRUE) (Single Database – BDU)*
- *European Commission (IMS; FTS)*

The PIAF-IT system has been the subject of very recent developments which have made it possible, as of November 2022, to enrich the reference information resources through consultation of the following databases:

- *National State Aid Register (RNA);*
- *Public Administration Database (BDAP);*
- *ReGiS management system for the National Recovery and Resilience Plan (NRRP);*
- *Bureau Van Dijk – ORBIS database.*

Q.2. Has any interoperability been developed between EU IT tools and national IT tools?

☒ YES

Q.3. If yes, with which tool?

- ☒ ARACHNE
- ☒ EDES
- ☒ IMS
- ☒ other (specify)

Q.4. To what end?

- ☒ Data enrichment
- ☒ Fine tune/refine red flags/risk indicators/risk scoring
- ☒ Other (specify)

Using and standardising the data available to the national and EU authorities;

Facilitating the exchange of information between all national and European actors for effective cooperation in the fight against fraud against the EU budget.

Q.5. How is digitalisation influencing the fight against fraud?

- ☒ Increasing prevention
- ☒ Increasing detection
- ☒ Reducing/simplifying administrative procedures
- ☒ Other (specify)

It ensures the traceability of information flows.

It makes it possible to ‘reconstruct’ the ‘infringement’ process, which is useful for strengthening the fight against fraud and to ensure ongoing monitoring of fraud risks and trends.

It allows an accurate risk analysis to be conducted.

3.16.4. Strengthen fraud risk analysis

Q.1 Have you implemented the recommendation?

☒ YES, fully

If you implemented fully the recommendation, can you please describe how you have done it? Can you share any specific findings? Please make a distinction between revenue and expenditure areas.

Contribution from AFCOS IT

In Italy, there is a well-established proactive approach to the issue of protecting the EU's financial interests through:

coordination and implementation of the national anti-fraud strategy.

Based on flexibility and dynamism, so as to adapt to the rapidly changing external environment, the national strategy relies on a highly structured system of institutions, judicial and administrative authorities, police forces, agencies, and management and control authorities – each responsible for specific sectors and/or individual phases of the anti-fraud cycle – which continually carry out joint analysis and hold discussions under the guidance and coordination of AFCOS, which is made up of members of all the national organisations concerned and is chaired by the Minister for European Affairs, the South, Cohesion Policies and the NRRP. Precisely because of these developments and in addition to the well-known qualities of the AFCOS, we would highlight the creation of the 'Network of Anti-fraud contact points of the NRRP', which, as part of the implementation of the National Recovery and Resilience Plan, is responsible for coordinating actions aimed at ensuring regular assessment of the risk of fraud, conflict of interest and double funding and defining effective and proportionate measures and actions. In order to support these objectives operationally, the 'General Anti-Fraud Strategy for the implementation of the National Recovery and Resilience Plan' was published in October 2022, describing the basic principles and general measures of the anti-fraud strategy necessary to ensure – in accordance with Article 22 of Regulation (EU) 2021/241 of 12 February 2021 – the correct use of Next Generation EU funds allocated to the NRRP. The document provides information on the anti-fraud 'system' put in place at national level to prevent, detect and correct cases of corruption, fraud and conflict of interest when using funding provided under the NRRP.

Analysis and assessment of fraud risks

The analysis and assessment of fraud risks and therefore the availability of computer databases and applications that can, by cross-checking and processing information, news and various elements, support the investigation of illegal practices and the selection of objectives are at the core of the national anti-fraud strategy.

In that respect, the project setting up the Integrated Anti-Fraud Platform (PIAF IT), which was launched in institutional collaboration with the Inspectorate General for Information Technology and Technological Innovation (IGIT) and the Inspectorate General for Financial Relations with the European Union (IGRUE) of the General Accounting Department of the Ministry of Economic Affairs and Finance has been further developed.

This IT tool fully complies with specific European legislative provisions and several sectoral recommendations of the European Commission, which stress the need to "design and focus audit and control activities on the basis of risk analysis and the development of IT tools" able to utilise the large amount of data available to the local authorities.

The aim of the platform is to enable data from various different national and European sources (including the Irregularity Management System (IMS) and the Financial Transformation System (FTS)) to be collected in a structured, digitalised and secure manner and organised in an integrated and harmonised way so as to enable all national administrations managing EU funds to have an immediate context for potential fraud strategies and the associated subjective and objective profiles, as well as to step up the exchange of information.

The platform is also intended to support the Commission's ARACHNE system for monitoring the NRRP.

For the sake of completeness, we would point out that all the national administrations dealing with the prevention and suppression of fraud, on both the revenue and expenditure side, have ad hoc databases and applications to carry out analyses and assessments of fraud risks for their respective areas of competence, thus ensuring interoperability.

Contribution of the Agency for Territorial Cohesion

The Agency for Territorial Cohesion (ATC) regularly monitors ARACHNE to support the sampling of operations for on-the-spot checks and to disseminate information on audit findings, in order to focus the intermediate bodies' own checks on any observations/irregularities found and recommendations made.

The ATC has distributed version 1.0 of the 'National Guidelines for the use of the EU's ARACHNE Anti-Fraud System', published by the Ministry of Economic Affairs and Finance, to the Managing Authorities and all the other bodies involved in various ways in the management and control process for the national and regional operational programmes in the context of the ERDF (certifying authorities, intermediate bodies and audit authorities).

With regard to the Agency for Territorial Cohesion's programmes, consideration was given to using the ARACHNE system and the new ex ante functionality, as suggested by the European Commission regarding the use of this IT system also as a tool for managing conflicts of interest during the selection of beneficiaries and, therefore, before funding is granted.

As part of the activities of the Joint Committee for the State – Regions and Autonomous Provinces, the Agency, as the national reference authority, contributed to the fraud risk assessment exercise of the ETC (European Territorial Cooperation) programmes for which it is responsible.

Contribution from the Ministry of Justice

Article 9 of Law No 127 of 4 August 2022 (European Delegation Law 2021), to bring national legislation into line with the Regulation on the European Public Prosecutor's Office – the body responsible for PIF offences – delegated to the Government the task of adopting one or more legislative decrees amending the rules on jurisdiction laid down in the Code of Criminal Procedure so as to concentrate in the district judicial offices the handling of proceedings for offences against the financial interests of the European Union in respect of which the European Public Prosecutor's Office may exercise its competence, irrespective of whether that competence is exercised, in order to make the activities of EDPs more efficient.

Contribution from the Ministry of Education

The MA of the 'National School Operational Programme' uses, for the purpose indicated, all the tools available: the Risk Self-Assessment Group, a general prevention tool which, specifically, acts as a link on issues and requirements relating to corruption prevention and transparency; the ARACHNE IT system; the Quality Review procedure for assessing the conformity of controls carried out.

3.17. Lithuania (LT)

3.17.1. Correct Transposition of the PIF Directive

Q.1. Has the Commission initiated infringement procedures against you for the incorrect transposition of the PIF Directive?

☒ NO

3.17.2. Participation in the EPPO

Q.1. Are you already participating in the EPPO?

☒ YES

3.17.3. Digitilising the fight against fraud

Q.1. Are you using any of the following IT systems in your fight against fraud?

☒ ARACHNE

Q.2. Has any interoperability been developed between EU IT tools and national IT tools?

☒ YES

Q.3. If yes, with which tool?

☒ ARACHNE

Q.4. To what end?

☒ Data enrichment

Q.5. How is digitalisation influencing the fight against fraud?

☒ Increasing prevention

☒ Increasing detection

☒ Reducing/simplifying administrative procedures

3.17.4. Strengthen fraud risk analysis

Q.1 Have you implemented the recommendation?

☒ YES, fully

If you implemented fully the recommendation, can you please describe how you have done it? Can you share any specific findings? Please make a distinction between revenue and expenditure areas.

If you implemented fully the recommendation, can you please describe how you have done it? Can you share any specific findings? Please make a distinction between revenue and expenditure areas.

- *Competence-based cooperation ensures that the EPPO is able to exercise all of the powers conferred on it;*

- *Comprehensive use of 'ARACHNE';*
- *By ensuring that the EU's financial interests are protected, fraud risk analysis is being improved and a methodology for evaluating criminal threats to the financial system is being developed.*

3.18. Luxembourg (LU)

3.18.1. Correct Transposition of the PIF Directive

Q.1. Has the Commission initiated infringement procedures against you for the incorrect transposition of the PIF Directive?

☒ NO

3.18.2. Participation in the EPPO

Q.1. Are you already participating in the EPPO?

☒ YES

3.18.3. Digitilising the fight against fraud

Q.1. Are you using any of the following IT systems in your fight against fraud?

☒ ARACHNE

☒ Cohesion (all programmes)

☒ Recovery and Resilience Facility

Q.2. Has any interoperability been developed between EU IT tools and national IT tools?

☒ YES

Q.3. If yes, with which tool?

☒ ARACHNE

Q.4. To what end?

☒ Data enrichment

Q.5. How is digitalisation influencing the fight against fraud?

☒ Increasing prevention

☒ Increasing administrative burden

Q.6. For any impact selected, can you provide any quantification?

There is no quantifiable data available

3.18.4. Strengthen fraud risk analysis

Q.1 Have you implemented the recommendation?

☒ YES, fully

If you implemented fully the recommendation, can you please describe how you have done it? Can you share any specific findings? Please make a distinction between revenue and expenditure areas.

Luxembourg takes a proactive approach in the fight against fraud. Due to its size and close geographical proximity of the different competent authorities, Luxembourg does permit a fast access and exchange of information to timely address emerging fraud risks. This includes also exchanging information with the Commission and other countries. To provide an example, Luxembourg customs informed during 2022 that it was able to uncover and seize 1.9 million cigarettes from smugglers thanks to information from their UK customs counterparts. A proactive approach has also been taken in the area of the Recovery and Resilience Facility, where an onsite meeting has been organized between the managing authority, AFCOS, the national audit authority and EPPO to establish a direct contact, share experiences and strengthen the anti-fraud cooperation.

3.19. Latvia (LV)

3.19.1. Correct Transposition of the PIF Directive

Q.1. Has the Commission initiated infringement procedures against you for the incorrect transposition of the PIF Directive?

☒ YES

Q.2. For the Member States having replied yes. Have you taken remedial action to modify national legislation?

☒ YES, for all launched infringements

Q.3. For the Member States having replied yes. By when do you expect to complete the modification of national legislation to correctly transpose the PIF Directive?

Latvia, in response to the EC initiated infringement procedure, indicated that during 2021 and 2022 it has already modified following national legislation:

- *the Criminal Law,*
- *the Law on Administrative Penalties for Offences in the Field of Administration, Public Order, and Use of the Official Language,*
- *the Law "On Taxes and Fees",*

thus ensuring that the violations indicated in the EC initiated infringement procedure have been eliminated. Since sending the EC this information, no new objections have been received from the EC regarding the implementation of the PIF Directive.

3.19.2. Participation in the EPPO

Q.1. Are you already participating in the EPPO?

☒ YES

3.19.3. Digitilising the fight against fraud

Q.1. Are you using any of the following IT systems in your fight against fraud?

☒ ARACHNE

☒ Cohesion (not all programmes) (*ETC not using, as technical solution for data transfer purposes to ARACHNE is being developed*)

☒ Rural Development Development (*in test mode*)

☒ EDES

☒ IMS (do not select if IMS is used only for reporting irregularities and fraud, as this is a legal obligation. Select if irregularities and fraud reported via IMS are used to perform risk analysis or other anti-fraud related activities)

☒ National dedicated anti-fraud IT tools

Q.2. Has any interoperability been developed between EU IT tools and national IT tools?

☒ NO

Q.3. If yes, with which tool?

☒ other (specify) *National EU Funds Management IT systems are linked with other national systems (e.g. Population Register of the Office of Citizenship and Migration Affairs; Information systems of the State Employment Agency for the registration of unemployed persons and registered vacancies; State Revenue Service's IT systems; The Disability Information System of the State Commission of Physicians for Health and Work Capacity Examination; State Regional Development Agency's IT systems; State Register of Addresses of the State Land Service)*

Q.4. To what end?

☒ Data enrichment

Q.5. How is digitalisation influencing the fight against fraud?

- ☒ Increasing prevention
- ☒ Increasing detection
- ☒ Reducing/simplifying administrative procedures

Q.6. For any impact selected, can you provide any quantification?

We cannot provide any quantification.

3.19.4. Strengthen fraud risk analysis

Q.1 Have you implemented the recommendation?

☒ YES, fully

If you implemented fully the recommendation, can you please describe how you have done it? Can you share any specific findings? Please make a distinction between revenue and expenditure areas.

In relation to expenditure area:

EU Funds Managing Authorities and Intermediate Bodies carry out regular risk assessment, using all available data, IT tools and information, including information provided by the EC, in order to take timely preventive actions to reduce fraud and corruption.

In relation to expenditure and revenue area:

AFCOS disseminated to the AFCOS Network all the information provided by the Commission in PIF report and other strategic analysis and targeted reports. All the information received from the Commission is constantly available in the AFCOS document platform (based on the MS SharePoint) and can be conveniently accessed and used by the AFCOS Network.

AFCOS elaborated IT tool based on the Methodology on typologies of crimes that can cause damage to the EU's financial interests. IT tool contains up-to-date red flags and typologies of fraud (including VAT fraud from the revenue area) and can be used by the AFCOS Network in order to help monitor fraud risks and trends.

3.20. Malta (MT)

3.20.1. Correct Transposition of the PIF Directive

Q.1. Has the Commission initiated infringement procedures against you for the incorrect transposition of the PIF Directive?

☒ YES

Q.2. For the Member States having replied yes. Have you taken remedial action to modify national legislation?

☒ YES, for all launched infringements

Q.3. For the Member States having replied yes. By when do you expect to complete the modification of national legislation to correctly transpose the PIF Directive?

Malta's Reply:

The necessary legislative changes are currently tabled in Parliament. The legislative process is expected to be finalised shortly.

3.20.2. Participation in the EPPO

Q.1. Are you already participating in the EPPO?

☒ YES

3.20.3. Digitilising the fight against fraud

Q.1. Are you using any of the following IT systems in your fight against fraud?

☒ ARACHNE

☒ Cohesion (all programmes)

☒ Recovery and Resilience Facility

Q.2. Has any interoperability been developed between EU IT tools and national IT tools?

☒ YES

Q.3. If yes, with which tool?

☒ ARACHNE

Q.4. To what end?

☒ Data enrichment

☒ Introduce new red flags/risk indicators

☒ Fine tune/refine red flags/risk indicators/risk scoring

Q.5. How is digitalisation influencing the fight against fraud?

☒ Increasing prevention

☒ Increasing detection

☒ Reducing/simplifying administrative procedures

Q.6. For any impact selected, can you provide any quantification?

Malta's Reply:

Digitalisation is considered as having a huge impact since it entails high usefulness to detect risks and alert stakeholders.

3.20.4. Strengthen fraud risk analysis

Q.1 Have you implemented the recommendation?

☒ YES, partly

If you implemented partially the recommendation, could you please explain why you think it was a partial implementation and why a full implementation was not possible? Please make a distinction between revenue and expenditure areas.

Malta's Reply:

In order to monitor fraud risks and trends, and address emerging risks in a timely manner, in 2022, the Internal Audit and Investigations Department (IAID) coordinated the drafting and publication of Malta's first National Risk Assessment (NRA) on Fraud and Corruption.

The document was published in December 2022 on IAID's website and can be accessed through the following link: <https://iaid.gov.mt/en/Pages/Co-ordinating-committee-.aspx>.

The NRA was prudently compiled on a high level through a collaborative approach involving all the members of the Co-ordinating Committee, set up in terms of Article 23 of the Internal Audit and Financial Investigations Act (Cap. 461 of the Laws of Malta) in order to 'co-ordinate the activities of, and to facilitate the exchange of information between, different entities charged with the protection and safeguarding of public funds'. The latter also include funds that Malta is required to manage under its international obligations. The list of the present members of the Co-ordinating Committee can be found on pages 9 and 10 of the NRA document. 7

The plan is that the NRA will be reviewed and updated if the need be on a biennial basis in order to reflect new developments, including regulatory and institutional changes, as well as the management of emerging risks.

3.21. Netherlands (NL)

3.21.1. Correct Transposition of the PIF Directive

Q.1. Has the Commission initiated infringement procedures against you for the incorrect transposition of the PIF Directive?

☒ NO

3.21.2. Participation in the EPPO

Q.1. Are you already participating in the EPPO?

☒ YES

3.21.3. Digitilising the fight against fraud

Q.1. Are you using any of the following IT systems in your fight against fraud?

- ☒ ARACHNE
- ☒ Cohesion (not all programmes)
- ☒ Recovery and Resilience Facility
- ☒ National dedicated anti-fraud IT tools

Q.2. Has any interoperability been developed between EU IT tools and national IT tools?

☒ NO

Q.5. How is digitalisation influencing the fight against fraud?

- ☒ Increasing prevention
- ☒ Increasing detection
- ☒ Increasing administrative burden

Q.6. For any impact selected, can you provide any quantification?

Increasing prevention/ detection:

In addition to the fact that these tools have a much larger data range and can provide insight into the entire population, data analysis is ideally suited to perform consistency checks on complex collections of related data and to identify exceptions more easily.

Increasing administrative burden:

We aren't fundamentally opposed to the use of a centralised IT system at EU level (ARACHNE) if it contributes to safeguarding the financial interests and interests of the EU. However, we are still very critical of how ARACHNE works in terms of user-friendliness, data protection and privacy, and the currently unclear added value of the system as a result of the problems we experience with it. In addition, it is found that current risk indicators identify false red flags and that ARACHNE generally does not meet the needs of the management authorities well and needs to undergo fundamental changes before it can meet expectations and needs. This results in increasing administrative burden.

3.21.4. Strengthen fraud risk analysis

Q.1 Have you implemented the recommendation?

☒ YES, partly

If you implemented partially the recommendation, could you please explain why you think it was a partial implementation and why a full implementation was not possible? Please make a distinction between revenue and expenditure areas.

If you implemented fully the recommendation, can you please describe how you have done it? Can you share any specific findings? Please make a distinction between revenue and expenditure areas.

If you implemented partially the recommendation, could you please explain why you think it was a partial implementation and why a full implementation was not possible? Please make a distinction between revenue and expenditure areas.

If you did not implement the recommendation, could you please explain why?

Fraud risks and the lawful use of funds (including EU funds) are important areas of focus within the Netherlands. In 2021 the Dutch internal audit paid extra attention to the mitigation of fraud risks and have separately included the opinion of fraud risks in the audit report accompanying the justification of the annual reports of the ministries. Overall, they concluded that the fraud risk management of the ministries is adequate.

Despite this finding of the internal audit service, a further professionalization of the fraud risk analysis is currently taking place. Due to digitization, more data is available. It is important that as much data as possible is taken into account when drawing up the fraud risk analysis. Where possible, databases are linked to each other.

Currently, not all revenue cycles work with specific fraud risks. However, risks are included with regard to the correctness, timeliness and completeness of the incoming cash flow, so that fraud risk is included. An office Security & Integrity is established to give the fraud risks and the associated measures a more prominent place within the already existing processes. At the moment this process is ongoing, that's why we mentioned the implementation as partly.

Finding expenditure

For an assessment of risks concerning related parties, the surrounding view within ARACHNE provides insight into the structure of the project partners. This allows risks to be identified aimed at parties/suppliers who are connected to the project partner. However, these risks can also be assessed through organisational structures and extracts from the Chamber of Commerce.

3.22. Poland (PL)

3.22.1. Correct Transposition of the PIF Directive

Q.1. Has the Commission initiated infringement procedures against you for the incorrect transposition of the PIF Directive?

☒ NO

3.22.2. Participation in the EPPO

Q.1. Are you already participating in the EPPO?

☒ NO

Q.2. For the Member States not participating yet. Are there plans to join the EPPO in the short-medium term?

☒ NO

3.22.3. Digitilising the fight against fraud

Q.1. Are you using any of the following IT systems in your fight against fraud?

☒ ARACHNE

☒ Recovery and Resilience Facility

☒ IMS (do not select if IMS is used only for reporting irregularities and fraud, as this is a legal obligation. Select if irregularities and fraud reported via IMS are used to perform risk analysis or other anti-fraud related activities)

☒ National dedicated anti-fraud IT tools

Q.2. Has any interoperability been developed between EU IT tools and national IT tools?

☒ NO

Q.5. How is digitalisation influencing the fight against fraud?

☒ Increasing prevention

☒ Increasing detection

☒ Reducing/simplifying administrative procedures

Q.6. For any impact selected, can you provide any quantification?

In the fight against fraud, prevention involves thorough checks on entities applying for EU funds and implementing projects cofinanced by the EU. Sources of information on this topic have so far been spread across many state registers, and using them has been a significant administrative burden. In the process of developing applications as part of the centralisation of recorded data on cohesion policy, an application similar to the economic information database has been created, which streamlines and speeds up the analysis process and at the same time provides the documentation necessary to ensure an audit trail. The application has not yet been used for long enough to provide accurate and reliable quantitative data.

Also in the agricultural sector, the procedures in place ensure the collection and use of data on detected fraud. Suspected fraud and confirmed fraud can be recorded in dedicated databases. These

databases are operated by all relevant institutions and entities carrying out delegated tasks and involved in the detection of irregularities and fraud. The databases are modified periodically as a result of new requirements to the extent necessary for the reporting of irregularities and the analysis of fraud. The data they contain make it significantly easier to carry out analyses, investigate and prevent fraud and identify suspected fraud. In addition to using the IMS system to send information on irregularities and fraud to the Commission, the information contained therein is used in the risk analysis carried out by the Managing Authority for the purpose of monitoring the proper implementation of the Rural Development Programme.

3.22.4. Strengthen fraud risk analysis

Q.1 Have you implemented the recommendation?

☒ YES, fully

If you implemented fully the recommendation, can you please describe how you have done it? Can you share any specific findings? Please make a distinction between revenue and expenditure areas.

Proactive measures to protect the European Union's financial interests have been taken and implemented in Poland for a number of years, notwithstanding the recommendation made in the 2021 PIF Report. On the expenditure side of the EU budget, this protection is achieved through the use of a variety of tools and mechanisms. In the Signals system, the institutions responsible for the implementation of cohesion policy operational programmes exchange information on potentially risky entities and other risks that have been identified. This mechanism is a response to the need to exchange information on warning signs of possible fraud. On the basis of a cooperation agreement between the National Public Prosecutor and the minister responsible for regional development (on the provision of information on ongoing and completed proceedings concerning projects carried out with cofinancing from European funds), there is a regular exchange of data on the beneficiaries of EU funds in respect of which investigations have been carried out. In addition, some bodies make use of the possibility to consult public prosecution service representatives if they urgently need data on ongoing proceedings. The cooperation agreement between the minister responsible for regional development and the Agency for Restructuring and Modernisation of Agriculture (ARiMR) formed the basis for cooperation in the implementation of cross-checks to detect and eliminate double financing of cohesion policy expenditure and expenditure under the 2014-2020 RDP and the 2014-2020 Fisheries OP. The agreement with the Central Anti-Corruption Bureau allows the information gathered in the electronic system supporting the implementation of operational programmes in the programming period 2014-20 to be provided to the organisational units of the Central Anti-Corruption Bureau by means of telecommunication. In addition, the Partnership Agreement Coordinating Authority organises annual conferences on controls and irregularities in the spending of Structural and Cohesion Funds, attended by representatives of the relevant institutions involved in the implementation and control of EU funds. The ARACHNE tool is used for the RRF. Selected representatives of OLAF and the Commission have also been granted access to the SL2014 main application to enable them to independently analyse the information on applicants, beneficiaries, expenditure cleared and checks carried out. New national IT tools dedicated to the new financial perspective have also been put in place:

e-Kontrolle (e-Controls) – an application to computerise controls of projects under cohesion policy programmes and reforms, investments and projects under the RRF;

SKANER (Scanner) – an application containing data on economic operators from internal databases and public registers, including their personal and capital links and data on projects cofinanced by EU funds carried out by these operators, and information on beneficial owners;

Kontrolle Krzyżowe (Cross-Checks) – a tool for grouping correlated invoices, where these can be used for double financing of expenditure.

In addition, the institutions at the level of each operational programme are required to draw up a document on how to prevent and deal with corruption and fraud, including conflicts of interest within the programme.

In the agricultural sector, an analysis of the risk of fraud is carried out each year in respect of the aid measures being operated, with the aim of identifying areas at risk of fraud, assessing effectiveness and, in specific cases, introducing control mechanisms to minimise the risk of fraud in the area of financial aid granted by the Paying Agency (Agency for Restructuring and Modernisation of Agriculture, ARiMR). As one of the elements used to verify cases at ARiMR, a list of signs of fraud has been introduced in order to raise awareness among employees of ARiMR at all stages of the administrative and control cycle as regards anomalies (signs) that could warrant suspicions of fraud and to increase the effectiveness of fraud prevention and detection. The list of signs is considered to be non-exhaustive and is updated on the basis of the results of fraud analysis, the results of other analytical activities concerning the fraud cases found, the results of audits and controls carried out at ARiMR and the Commission's reports and analyses.

The procedures in place to assess whether financial assistance is correctly granted and used ensure that all information (including anonymous information) is verified and that all available sources are used in cases of suspected fraud. In addition, ARiMR cooperates with law enforcement authorities in the framework of its investigations, including by carrying out inspection activities at the request of the public prosecution service. ARiMR also provides all information and the required documents and cooperates with OLAF in connection with administrative investigations carried out by the Office.

Analytical activities for the National Revenue Administration (KAS) with regard to revenue are carried out by the Strategic Analysis Centre at the Katowice Regional Revenue Administration Office. These activities are implemented by means of an exchange of information with the Commission and the Member States via the CRMS2 or AFIS systems, and with other Regional Revenue Administration Offices by circulation of internal information in the National Revenue Administration. When messages concerning RIF or AM are received, the information they contain is analysed. Where a risk is identified, the information is entered in the integrated risk analysis system, with a description of the case and an indication of the specific risk area. Depending on the nature of the information indicated in the messages concerning RIF and AM, analytical activities are undertaken on the basis of the National Revenue Administration's operational systems and data are compiled and sent as necessary to OLAF and the Regional Revenue Administration Office (with recommendations for specific actions to be taken). There are also reservations at central level (central risk profiles) in the integrated risk analysis system, which provides a risk analysis service for the National Revenue Administration's operational systems. Feedback to the Commission and the Member States on actions taken on the basis of information received, the reservations introduced in the IT systems, the results of checks, recoveries, etc. are submitted via the CRMS2 and AFIS systems. The relevant information is also forwarded to other authorities, e.g. the public prosecution service.

3.23. Portugal (PT)

3.23.1. Correct Transposition of the PIF Directive

Q.1. Has the Commission initiated infringement procedures against you for the incorrect transposition of the PIF Directive?

☒ YES

Q.3. For the Member States having replied yes. By when do you expect to complete the modification of national legislation to correctly transpose the PIF Directive?

The process is under way and is expected to be concluded shortly.

3.23.2. Participation in the EPPO

Q.1. Are you already participating in the EPPO?

☒ YES

3.23.3. Digitilising the fight against fraud

Q.1. Are you using any of the following IT systems in your fight against fraud?

☒ ARACHNE

☒ Cohesion (not all programmes)

☒ Recovery and Resilience Facility

☒ EDES

☒ IMS (do not select if IMS is used only for reporting irregularities and fraud, as this is a legal obligation. Select if irregularities and fraud reported via IMS are used to perform risk analysis or other anti-fraud related activities)

☒ other (specify) (*eInforma – IFA*)

Q.2. Has any interoperability been developed between EU IT tools and national IT tools?

☒ NO

Q.5. How is digitalisation influencing the fight against fraud?

☒ Increasing prevention

☒ Increasing detection

☒ Reducing/simplifying administrative procedures

3.23.4. Strengthen fraud risk analysis

Q.1 Have you implemented the recommendation?

☒ YES, fully *as regards the fight against fraud and tax and customs duty evasion*

☒ YES, partly *with regard to the control of European funds*

If you implemented fully the recommendation, can you please describe how you have done it? Can you share any specific findings? Please make a distinction between revenue and expenditure areas.

The Portuguese Tax and Customs Authority uses all available information – from both internal and external sources – that is relevant for checking operators and activities in order to prevent, detect and investigate VAT fraud (among other revenue sources). As regards VAT and combating VAT fraud, the use of the administrative cooperation instruments provided for in Council Regulation (EU) No 904/2010 of 7 October 2010 is particularly important.

If you implemented partially the recommendation, could you please explain why you think it was a partial implementation and why a full implementation was not possible? Please make a distinction between revenue and expenditure areas.

In the area of expenditure, the national anti-fraud strategy (NAFS) was revised. It includes a 5-year action plan setting out concrete fraud risk analysis measures.

3.24. Romania (RO)

3.24.1. Correct Transposition of the PIF Directive

Q.1. Has the Commission initiated infringement procedures against you for the incorrect transposition of the PIF Directive?

☒ YES

Q.2 For the Member States having replied yes. Have you taken remedial action to modify national legislation?

☒ YES, but not for all launched infringements ¹⁶

3.24.2. Participation in the EPPO

Q.1. Are you already participating in the EPPO?

☒ YES

3.24.3. Digitilising the fight against fraud

Q.1. Are you using any of the following IT systems in your fight against fraud?

☒ ARACHNE

☒ Cohesion (all programmes)

☒ Rural Development

☒ IMS (do not select if IMS is used only for reporting irregularities and fraud, as this is a legal obligation. Select if irregularities and fraud reported via IMS are used to perform risk analysis or other anti-fraud related activities)

☒ other (specify) – IACS (*integrated administration and control system*), a technical tool set up for the management and control of single payment applications submitted by farmers

☒ National dedicated anti-fraud IT tools

Q.2. Has any interoperability been developed between EU IT tools and national IT tools?

☒ YES

Q.3. If yes, with which tool?

☒ ARACHNE

Q.4. To what end?

☒ Data enrichment

☒ Fine tune/refine red flags/risk indicators/risk scoring

Q.5. How is digitalisation influencing the fight against fraud?

☒ Increasing prevention

☒ Increasing detection

☒ Decreasing detection

¹⁶ In 2023, Romania reportedly took action to address all launched infringements.

☒ Reducing/simplifying administrative procedures

3.24.4. Strengthen fraud risk analysis

Q.1 Have you implemented the recommendation?

☒ YES, fully

If you implemented fully the recommendation, can you please describe how you have done it? Can you share any specific findings? Please make a distinction between revenue and expenditure areas.

On the expenditure side:

Managing authority (MA) - 'Competitiveness' OP: In accordance with the legal provisions laid down in Article 125 of Regulation (EU) No 1303/2013 (relating to 'Competitiveness' OP 2014-2020) and Regulation (EU) No 1060/2021 (relating to 'Smart Growth, Digitalisation and Financial Instruments' OP): the managing authority shall be responsible for managing the operational programme in accordance with the principle of sound financial management. As regards the management of the operational programme, the managing authority shall put in place effective and proportionate anti-fraud measures taking into account the risks identified. As a result, the Directorate-General for Smart Growth and Digitalisation (DGCID) carried out the fraud risk assessment for 2022.

Irregularities (including fraud) are closely monitored until the debts owed by beneficiaries are recovered. In order to correctly address this issue, in particular as regards suspicions of irregularities and the way they are monitored, the MA has implemented several levels of checks, such as: use of internal operational procedures ('Irregularity Management', 'Major Risk Assessment' and 'Fraud Risk Assessment'). They all thoroughly describe the activities that are mandatory for the sole purpose of successfully identifying, sanctioning and monitoring all cases of irregularities.

In addition to the aforementioned procedures, the MA also has access to ARACHNE. This is a risk-scoring tool developed by the Commission that aims to support the MA's efforts to effectively and efficiently identify the riskiest projects, contractors and beneficiaries, as required to comply with Article 125(4)(c) of Regulation (EU) No 1303/2013.

MA - 'Large infrastructure' OP

Within the DGPDD (Directorate-General for the Sustainable Development Programme), the Operational Procedure PO.DGPDD.30 'Fraud Risk Assessment', Edition I, Revision 0 was drawn up on the basis of the EC's anti-fraud guidance issued in 2014.

At the same time, a fraud risk assessment was carried out between 14-18 November 2022. As a result, an INFORMATION NOTE on the results and conclusions of the internal fraud risk assessment and the actions and measures proposed for LIOP 2014-2020 was drawn up on 4 January 2023.

The fraud risk assessment covers four key processes that are considered to be most exposed to the fraud risks identified in the implementation of LIOP 2014-2020, namely:

- *selecting and evaluating projects (funding applications);*
- *the technical and procurement aspects of implementing and auditing operations;*
- *certifying/checking costs and making payments;*
- *establishing irregularities and preventing, detecting and reporting fraud.*

The risk assessment concluded that all fraud risks that may arise within the MA for the LIOP are already at an acceptable level, which allows the MA to carry out its activities. The assessment team considers that the existing forms of control are sufficient, that no additional checks or specific anti-fraud measures are required, and that it is not necessary to draw up a fraud risk mitigation plan. However, the assessment team recommends close monitoring of the activities carried out within the

MA for the LIOP in order to ensure that the tolerable level of fraud risk is maintained and to identify potential new fraud risks.

MA - 'Technical Assistance' OP

For the purpose of the fraud risk analysis, the MA TAOP team took into account the controls/checks carried out in accordance with the operational procedures and the collaboration protocols concluded with the relevant verification institutions, also taking into account the use of the ARACHNE system, and analysed the impact of potential risks leading to malfunctions in the TAOP 2014-2020 management and control system. The analysis of the assessment result thus showed that the MA TAOP management and control system is functioning well and that the level of confidence in the verifications carried out by the managing authority can be considered as high.

DG PECU (Directorate-General for European Human Capital Programmes)

In order to strengthen the fraud risk analysis, DG PECU has taken a proactive approach to protecting the EU's financial interests by:

- using data from all available sources,*
- analysing data and exchanging information,*
- cooperating with law enforcement authorities (DLAF - the Anti-Fraud Department, DNA - the National Anti-corruption Directorate, EPPO - the European Public Prosecutor's Office, ANI - the National Integrity Authority),*
- and carrying out the fraud risk assessment, which was completed when the note on the results of the assessment of fraud risks identified by DG PECU as concerns 'Human Capital' OP and the action plan to mitigate fraud risks were approved, in accordance with the Fraud Risk Assessment Operational Procedure.*

National recovery and resilience plans

As regards the protection of the EU's financial interests, Romania has taken the following measures linked to the RRF:

Legislative measures: (a) implementing the National Anti-Fraud Strategy, the National Anti-Corruption Strategy, Law No 129/2019 on preventing and fighting money-laundering and terrorist financing; (b) setting up the institutional and financial framework to manage European funds allocated to Romania under the Recovery and Resilience Facility, and establishing the legal framework to prevent, check and detect irregularities or double financing, and serious irregularities in obtaining and using RRF funds, including the relationship between institutions managing RRF funds and authorities in charge of detecting serious irregularities, with GEO (Government Emergency Orders) Nos 155/2020, 124/2021 and 70/2022.

Administrative, organisational and operational measures: (a) development by the Ministry of Investment and European Projects (MIPE) in cooperation with the Special Telecommunications Service (STS) of a management and control IT system meeting the requirements laid down in Article 22(2)(d) of Regulation (EU) 2021/241. The IT system is interconnected with the databases of national institutions managing the data on the actual beneficiaries; (b) operational procedures for managing and preventing risks of serious irregularities, and operational procedures to track and recover debts

In order to carry out its preventive and control tasks, the Directorate-General for Fisheries (MA for the Operational Programme for Fisheries and Maritime Affairs (POPAM)) cooperates with the contact institution for the European Anti-Fraud Office – the Anti-Fraud Department (DLAF), and with other national relevant institutions.

DLAF is in constant contact with the managing authorities for EU funds in order to assess the fraud risk, and monitors and centralises the briefing notes drawn up by the MAs on the assessment results.

The results have been taken into account in the development of the National Anti-Fraud Strategy.

On the revenue side:

AVR (the Romanian Customs Authority)

The reorganisation of the Romanian customs administration started at the end of 2021 and was implemented at the beginning of April 2022:

- *since April 2022, the Romanian Customs Authority has been subordinated to the Ministry of Finance; there are seven regional customs directorates and 91 inland and border customs offices operating under the Authority's aegis; a total of 3 060 posts have been approved by government decision;*
- *mobility measures were taken and staff from mobile teams and from inland customs offices were posted to customs offices at the border with the Republic of Moldova and Ukraine, as well as in the Black Sea ports;*
- *in accordance with GEO No 103 of 30 June 2022 on measures to increase the border control capacity of the Romanian Customs Authority, 324 posts were added to the establishment plan for a fixed period - until the situation leading to the massive flow of goods and people at the Romanian border with Ukraine and the Republic of Moldova and in the Black Sea ports is resolved, but not more than three years from the date of entry into force of the Emergency Order;*
- *in early 2022, the Minister of Finance approved a Strategy on the Romanian Customs Authority's reform for 2022-2024, with the following strategic objectives:*
 - *facilitating legitimate trade and improving services for all parties involved;*
 - *increasing digitalisation at local customs authority level;*
 - *increasing the EU's external border's security;*
 - *strengthening the capacity to prevent and fight cross-border crime and customs and tax fraud;*
 - *increasing efficiency, visibility, transparency and access to the business environment;*
 - *strengthening the administrative capacity of the customs authority in accordance with European (and international) standards.*

The Romanian Customs Authority is responsible for customs control at Romania's and the EU's external border, for customs control of import, export and transit operations, for post-clearance checks and for unannounced inspections to monitor and control activities linked to the production, possession, movement and use of excise goods. European and international standards on tariff classification, origin and customs value have been implemented and are applied at national level, and there are ongoing projects to develop customs IT systems under the EU's Multi-Annual Strategic Plan for Electronic Customs (MASP-C).

Since 2010, the Romanian customs administration has been using the national IT application RMF-RO (Risk Management Framework-RO) to carry out specific risk management and risk treatment activities in the area of customs in order to identify, prevent and fight customs fraud when import, export or transit operations are performed and when legal safety and security provisions are implemented. Risk profiles (a predefined combination of risk indicators that have been collected, analysed and ranked) are developed at all levels of the customs authority (local, regional and central). They are only implemented in the RMF-RO system at central level.

The RMF-RO system has incorporated the criteria and standards for financial risks adopted by the European Commission in 2018 (in the Financial Risks Criteria and Standards Implementing Decision (the 'FRC Decision') - Commission Implementing Decision C(2018)3293), and is using risk profiles based on risk indicators established at EU level.

At the same time, all the levels of the customs authority (local, regional and central) are using the customs risk management system developed by DG TAXUD (CRMS2 – Customs Risk Management

System 2), and the AFIS system developed by OLAF. The information exchanged through this system between Member States' administrations and with the relevant Commission departments is used by customs officials in charge of risk analysis to develop new risk profiles and to order specific controls and checks (during clearance of goods or afterwards).

The exchange of risk information with other Romanian law enforcement authorities (the National Tax Administration Agency (ANAF), the police, the border police, the public prosecutor's office, the Environmental Guard, sanitary-veterinary and phytosanitary authorities, etc.), based on cooperation protocols or memoranda of understanding, takes place through mutual access to databases and the use of customs officers seconded to the Centre for International Police Cooperation - National Focal Point or to the National Passenger Information Unit within the General Border Guard Inspectorate (IGPF). Moreover, at central level there is also a body dedicated to coordinating and ensuring mutual administrative assistance on customs and excise matters. This body implements Regulation (EC) No 515/1997 on mutual assistance between the administrative authorities of the Member States and cooperation between the latter and the Commission so as to ensure the correct application of the legislation on customs and agricultural matters, as amended, Council Regulation (EU) No 389/2012 of 2 May 2012 on administrative cooperation in the field of excise duties and repealing Regulation (EC) No 2073/2004, the SELEC Convention and the Naples II Convention, as well as international agreements, conventions and treaties to which Romania is a party (in the framework of mutual customs assistance arrangements with non-EU countries).

In 2022, the Romanian customs administration continued to be actively involved in implementing the 2022-2025 EMPACT EU Policy Cycle, and also participated in the activities carried out in the framework of the joint customs operations (JCOs) organised by OLAF, WCO, INTERPOL, and EUROPOL.

As regards the prevention and fight against illicit trafficking in cigarettes and tobacco products, operational cooperation with other Romanian law enforcement authorities (ANAF, the police, the border police, the public prosecutor's office) continued. The checks carried out in close cooperation with these authorities to fight tobacco products smuggling resulted in a significant decrease in the estimated consumption level of illicit cigarettes in Romania, which dropped from an average of 8.7% of the total cigarette consumption in 2021 to an average of 7.1% in 2022, a record low level for the past 15 years. We would point out that with every percentage point that goes to the legal market, the State budget receives EUR 35-40 million. In 2022, the Romanian Customs Authority's central and local customs supervision and control bodies seized over 19.4 million cigarettes and 27 tons of tobacco.

3.25. Sweden (SE)

3.25.1. Correct Transposition of the PIF Directive

Q.1. Has the Commission initiated infringement procedures against you for the incorrect transposition of the PIF Directive?

☒ YES

Q.2. For the Member States having replied yes. Have you taken remedial action to modify national legislation?

☒ YES, for all launched infringements

Q.3. For the Member States having replied yes. By when do you expect to complete the modification of national legislation to correctly transpose the PIF Directive?

The Commission has stated in a formal notification that Sweden has failed to correctly incorporate articles 3.2 d i, 3.2 d iii and article 5.2 compared with article 3.2 a and 3.2 b, into its national legislation.

Before the Government can draw up a legislative proposal, the matter must be analysed. In June 2022, the Swedish Government decided to appoint a commission of inquiry to, inter alia, propose measures regarding the first part of the formal notice from the Commission (3.2 d i and 3.2 d iii). The inquiry will submit its report by 31 August 2023.

When it comes to the second part of the formal notice (5.2 compared with article 3.2 a and 3.2 b), the Government has proposed, in a proposal referred to the Council of Legislation, that attempting to commit subsidy abuse or gross subsidy abuse should be criminalised. The amendments are proposed to enter into force on 1 June 2023.

3.25.2. Participation in the EPPO

Q.1. Are you already participating in the EPPO?

☒ NO

Q.2. For the Member States not participating yet. Are there plans to join the EPPO in the short-medium term?

☒ YES

Q.3. If YES, when do you expect to finalise the procedure?

The Government is currently working on a proposal containing the necessary legislation to enable Sweden to join the EPPO as soon as possible, provided endorsement from Parliament.

3.25.3. Digitilising the fight against fraud

Q.1. Are you using any of the following IT systems in your fight against fraud?

☒ National dedicated anti-fraud IT tools

Q.2. Has any interoperability been developed between EU IT tools and national IT tools?

☒ NO

3.25.4. Strengthen fraud risk analysis

Q.1 Have you implemented the recommendation?

☒ NO

If you did not implement the recommendation, could you please explain why?

If you implemented fully the recommendation, can you please describe how you have done it? Can you share any specific findings? Please make a distinction between revenue and expenditure areas.

If you implemented partially the recommendation, could you please explain why you think it was a partial implementation and why a full implementation was not possible? Please make a distinction between revenue and expenditure areas.

If you did not implement the recommendation, could you please explain why?

Sweden works proactively to protect the EU's financial interests, for example by closely following recommendations and reports produced by OLAF, the Court of Auditors and the Commission, etc. institutions and best practices in the other Member States.

Currently, there is no national common database for Swedish authorities handling EU funds. In this context, it must also be held that the Swedish judiciary's databases are not open databases and that there is legislation that prevents such data from being used outside the judicial system.

The Swedish government decided in December 2021 to appoint an inquiry regarding the effective and efficient management of EU funds in Sweden. The assignment not only concerns the management of EU funds, but the inquiry will also make proposals for an organizational structure and division of responsibilities that will enable a more effective, efficient and legally secure management of EU funds, which at the same time lives up to the requirements set by the EU. The study, called "An effective and efficient management of EU funds Dir 2021:109", will submit a final report in December 2023.

3.26. Slovenia (SI)

3.26.1. Correct Transposition of the PIF Directive

Q.1. Has the Commission initiated infringement procedures against you for the incorrect transposition of the PIF Directive?

☒ YES

Q.2. For the Member States having replied yes. Have you taken remedial action to modify national legislation?

☒ YES, but not for all launched infringements

Q.3. For the Member States having replied yes. By when do you expect to complete the modification of national legislation to correctly transpose the PIF Directive?

The Act amending the Penal Code is expected to be published in the official gazette (Uradni List Republike Slovenije) in February 2023. Regarding the second and third comments: the Government of Slovenia explained in its reply to the letter of formal notice that it believes the regulation in Slovenia are fit for purpose and no further changes are necessary.

3.26.2. Participation in the EPPO

Q.1. Are you already participating in the EPPO?

☒ YES

3.26.3. Digitilising the fight against fraud

Q.1. Are you using any of the following IT systems in your fight against fraud?

☒ ARACHNE (*Office for Cohesion Policy, Agency of the Republic of Slovenia for Agricultural Markets and Rural Development (ARSKTRP)*)

☒ Cohesion (all programmes)

☒ Rural Development

☒ IMS (do not select if IMS is used only for reporting irregularities and fraud, as this is a legal obligation. Select if irregularities and fraud reported via IMS are used to perform risk analysis or other anti-fraud related activities)

☒ other (specify) *GVIN, e-Bonitete, AJPES (Agency of the Republic of Slovenia for Public Legal Records and Related Services), MFERAC (Office for Cohesion Policy), ERAR,*

Q.2. Has any interoperability been developed between EU IT tools and national IT tools?

☒ YES

Q.3. If yes, with which tool?

☒ ARACHNE

Q.4. To what end?

☒ Data enrichment

☐ Streamline and automatise the reporting of irregularities

- ☒ Introduce new red flags/risk indicators
- ☐ Fine tune/refine red flags/risk indicators/risk scoring
- ☐ Other (specify)

Q.5. How is digitalisation influencing the fight against fraud?

- ☒ Increasing prevention
- ☒ Decreasing prevention
- ☒ Increasing detection
- ☒ Decreasing detection
- ☒ Other (specify)

Reply from URSOO:

- *Improving risk management through data mining*
- *Improving the performance of the early detection and exclusion system*
- *Improving the effectiveness and quality of checks and audits*
- *Strengthening risk analysis for fraud*

Q.6. For any impact selected, can you provide any quantification?

3.26.4. Strengthen fraud risk analysis

Q.1 Have you implemented the recommendation?

☒ YES, fully (*reply from FURS (Financial Administration of the Republic of Slovenia) and the Government Office for Development and European Cohesion Policy (SVRK) - Office for Cohesion Policy,*
Reply from URSOO)

If you implemented fully the recommendation, can you please describe how you have done it? Can you share any specific findings? Please make a distinction between revenue and expenditure areas.

Reply from FURS:

The Financial Administration of Slovenia (FURS) has assumed a proactive role in protecting the EU's financial interests by analysing and exchanging data and information for the purpose of managing risks associated with customs and VAT. Details on how FURS protects the EU's financial interests are provided below.

The exchange of vital data and information happens at EU level. This data includes data on risks arising from the systems, such as CRMS, AFIS, RAPEX, RASFF, TRACES NT, EUROFISC and TNA. FURS analyses these data and uses them to create risk profiles, which apply to checks preceding release into free circulation, ex-post checks and inspections. Risk-related information is, where required, forwarded to the other competent authorities (national or EU) for further processing.

We would single out data obtained from the Anti Fraud Information System (AFIS), which is most commonly used as a gateway to the following databases and tools:

AMT (Automated Monitoring Tool) or Theseus (Joint Research Centre – JRC). The database in these applications contains cleaned average prices (CAPs) and is incorporated in FURS' databases on a monthly basis. By comparing CAPs and the actual import data, the IT system calculates and identifies

suspicion of undervalued goods. Where a suspicion is established, this triggers risk profiles for release into circulation, which is followed up by a verification of the customs value of the goods.

Container Status Messages (CSMs), the JRC's ConTraffic database and Sea Searcher facilitate container and ship tracking to combat fraud related to the provenance of goods or the avoidance of payment of anti-dumping and countervailing duties. FURS obtains data from these applications by running manual queries.

Dun & Bradstreet – Global Reference Solution (previously Orbis) makes it possible to check whether a company referred to in customs papers or procedures actually exists. FURS obtains data from these applications by running manual queries.

Given the international dimension of fraud, information obtained by FURS from the other Member States through international exchange mechanisms and OLAF plays a vital role in protecting the EU's financial interests.

Regulation (EC) No 515/97 of 13 March 1997 provides for mutual assistance between the administrative authorities of the Member States and cooperation between the latter and the Commission to ensure the correct application of the law on customs and agricultural matters FURS processes OLAF's mutual assistance messages and mission reports on an ongoing basis and uses them to create systemic measures involving the creation of risk profiles for checks preceding release into free circulation, and carry out ex-post checks and inspections. The findings are submitted to OLAF.

Where there is suspicion, with regard to imports from third countries, that supplier documents are forged or unauthentic, FURS sends international letters of request to third-country customs authorities in accordance with bilateral or multilateral agreements and protocols (Slovenia vis-à-vis a third country or EU vis-à-vis a third country).

In addition, available tax data exchanged in accordance with Council Regulation (EU) No 904/2010 of 7 October 2010 on administrative cooperation and combating fraud in the field of value added tax are used for the purpose of protecting the EU's financial interests. The main source of data is Eurofisc's tool TNA. Data on individual liable entities associated with risk (Eurofisc qualification) are transferred into FURS' databases and used primarily to generate risk profiles for checks preceding release into free circulation but also for identifying subjects of future ex-post checks and inspections. The data from Eurofisc are particularly important for monitoring the conduct of customs procedures Nos 46 and 63. A new form of Eurofisc data exchange called Follow-Up Action is used to identify (more complex) misuse of customs procedures more quickly.

FURS reports all instances of suspected crime to the police and/or the competent prosecutor's office. FURS closely cooperates with law enforcement authorities; in complex cases involving an international component all the authorities cooperate and exchange information with one another since the very beginning in the form of specialised investigation teams. Where a crime harms the financial interests of the EU, FURS cooperates with the EPPO by reporting crime or submitting data required for prosecution in another Member State.

We should like to point out that we cooperate with the Office for the Prevention of Money Laundering and Terrorist Financing, exchanging information on suspicious transactions, which is a major input for risk analysis

Reply from the Office for Cohesion Policy: Fully implemented since, in addition to ARACHNE, we also use national databases (GVIN, e-Bonitete, AJPES, MFERAC), which are authorised for collecting, processing and keeping public annual and other end-of-year reports. We use our data tools to examine general, accounting and other financial data on a selected entity. This guarantees the protection of the financial interests of the EU and Slovenia.

Reply from URSOO:

adoption of the Strategy of the coordination body of the Recovery and Resilience Facility for fighting fraud and regular updates to the action plan;

cooperation with law enforcement authorities (police, EPPO);

training courses on integrity and combating fraud;

organising training on the protection of the EU's financial interests;

informing the competent authorities on training and education activities to do with the protection of the EU's financial interests.

3.27. Slovakia (SK)

3.27.1. Correct Transposition of the PIF Directive

Q.1. Has the Commission initiated infringement procedures against you for the incorrect transposition of the PIF Directive?

☒ YES

Q.2. For the Member States having replied yes. Have you taken remedial action to modify national legislation?

☒ YES, for all launched infringements

Q.3. For the Member States having replied yes. By when do you expect to complete the modification of national legislation to correctly transpose the PIF Directive?

The legislative changes regarding the modification of the national legislation are in the legislative procedure. The modification shall enter into force by 1/1/2022.

3.27.2. Participation in the EPPO

Q.1. Are you already participating in the EPPO?

☒ YES

3.27.3. Digitilising the fight against fraud

Q.1. Are you using any of the following IT systems in your fight against fraud?

☒ ARACHNE

☒ All EU funds and programmes (Cohesion, Rural Development, Recovery and Resilience Facility)

☒ Cohesion (all programmes)

☐ Cohesion (not all programmes)

☒ Rural Development

☒ Recovery and Resilience Facility

☒ EDES

☒ IMS (do not select if IMS is used only for reporting irregularities and fraud, as this is a legal obligation. Select if irregularities and fraud reported via IMS are used to perform risk analysis or other anti-fraud related activities)

☒ other (specify)

1. *online database Index Podnikatela ([www. https://www.indexpodnikatela.sk/](https://www.indexpodnikatela.sk/)) that is actually a tool to link 26 different databases to crosscheck connections between procurement officials and bidders.*
2. *online database Foaf (<https://foaf.sk/>) that is actually a tool to provide visualization of company connections.*
3. *Anti-bureaucratic Portal OverSi (Portál OverSi (gov.sk))*
4. *Register of legal entities, entrepreneurs and public authorities: <https://rpo.statistics.sk>*
5. *Portal for registration and monitoring of state aid: <https://semp.kti2dc.sk/>*
6. *Insolvency Register: <https://ru.justice.sk/ru-verejnost-web/>*
7. *Central register of executions : www.cre.sk*
8. *List of legally convicted legal entities*

☒ National dedicated anti-fraud IT tools

Q.2. Has any interoperability been developed between EU IT tools and national IT tools?

☒ YES

Q.3. If yes, with which tool?

☒ ARACHNE

☒ IMS

Note:

ARACHNE: The transfer of data from relevant national systems to ARACHNE is not automated on a software level, but has been implemented as a manual and regular process.

IMS: there is a partial interoperability between IMS and national IT Monitoring System for ESIF (ITMS2014+), but full interoperability has not been reached yet.

Q.4. To what end?

☒ Data enrichment

☒ Streamline and automatise the reporting of irregularities

☒ Fine tune/refine red flags/risk indicators/risk scoring

Q.5. How is digitalisation influencing the fight against fraud?

☒ Increasing prevention

☒ Increasing detection

☒ Reducing/simplifying administrative procedures

Q.6. For any impact selected, can you provide any quantification?

We do not have any data to quantify the impact of the use of selected IT tools in the fight against fraud.

3.27.4. Strengthen fraud risk analysis

Q.1 Have you implemented the recommendation?

☒ YES, fully

If you implemented fully the recommendation, can you please describe how you have done it? Can you share any specific findings? Please make a distinction between revenue and expenditure areas.

The Office of the Government of the Slovak Republic is via its Section of Control, National Office for OLAF (department), responsible for ensuring and coordinating the protection of the EU's financial interests in the Slovak Republic. If the National Office for OLAF receives materials, analyses and reports from the Commission (OLAF) containing useful information in the anti-fraud area, these documents are distributed to the AFCOS network partners in order to be considered in their fraud risk analysis, if relevant. The National Office for OLAF also elaborates its own materials and analyses (e.g. Annual Report on Irregularities), which are distributed to the relevant national authorities within the AFCOS network.

In addition, the exchange of information on emerging risks and fraud trends also takes place during training activities in the area of the protection of the EU's financial interests organised by the National Office for OLAF, which are attended also by the representatives of the law enforcement

bodies (as lectures and also as participants) and cover both expenditure and revenue side of the EU budget.

In order to prevent, detect and investigate fraud and other irregularities, national authorities also use wide range of available EU and national databases, exchange relevant information and provide mutual assistance.

With respect to this questionnaire, the Office of the Government of the Slovak Republic also contacted AFCOS network partners (national authorities, including managing authorities, certifying authority, control bodies etc.) in order to gather relevant information. Below please find detailed replies as provided by some of them:

Expenditure area:

The Ministry of Health of the Slovak Republic, as an intermediary body, fully accepted and implemented the European Commission's recommendation to deal with the risks of fraud based on the 2014 guideline, as well as the guideline that was a response to the situation and addresses anti-corruption measures in the context of CRII/CRII+ and the REACT-EU program. The Ministry has drawn up tables based on fraud risks identified by the EC (also in connection with the pandemic situation), proposed measures, action plans and makes an annual evaluation of fulfilled measures. According to the obligation arising from the Statute and Rules of procedure of the Working group for IROP risk management, the governing body is informed about the activities and outputs of the working group.

The Ministry of Finance of the Slovak Republic, acting as Certifying Authority (CA) has developed a risk management system resulting from CA activities and its management and control systems, including the processes of identification, analysis and assessment of risks, their solutions and measures taken to eliminate them, including permanent monitoring and evaluation. This system is subject to regular analysis and updating as of 30.11. of the respective year. The risk analysis system also includes identified risks of possible corruption and fraud and "sensitive positions", including measures to prevent the occurrence of corruption and fraud at CA.

The Ministry of Agriculture and Rural Development of the Slovak Republic informed, that the Agricultural Paying Agency has adopted internal guidelines for the prevention of fraud and irregularities, which specify obligations and processes in relation to fraud and communication with the relevant authorities.

The Ministry of Investments, Regional Development and Informatization of the Slovak Republic stated that the employees of the Managing Authority for Integrated Regional Operational Programme (IROP), as well as the intermediate bodies (IB), responsible for the administrative verification of the requests for a non-refundable financial contribution, control and implementation of projects, work with the ARACHNE and EDES information systems and use other available national registers and databases in order to protect the financial interests of the EU and prevent fraud. Follow-up processes related to identification of possible fraud, which may lead to the identification of irregularities, or to the sending of an initiative to other entities involved in the protection of financial interests (National Office for OLAF, law enforcement authorities, EPPO) are ensured in cooperation with the control department of IROP section, which covers further communication and exchange of information. Also, in conditions of the Managing Authority for IROP, the Working Group for Risk Management meets every year, which, among other things, deals with monitoring the risks of fraud and their occurrence within the program. All procedures are incorporated in the internal management documentation. 8 IB for Priority Axis (PA) 7 of the Operation Programme Integrated Infrastructure (OPII) in accordance with the European structural and investment funds Management System for detecting fraud risks uses a fraud risk self-assessment tool in cooperation with Managing Authority, i.e. matrix - catalog of risks. The stated IB PA7 OPII fraud risk analysis is carried out once a year and is carried out in

accordance with the guideline EGESIF_14-0021-00 16/06/2014", issued by the European Commission.

The Managing Authority for the cross border Cooperation Interreg SK-CZ and Interreg SK-AT has established a Risk Management Working Group which reviews on a regular annual basis the risks and the effectiveness of measures to eliminate them, including supporting tools for verifying the economy and eligibility of expenditures. The appropriateness and effectiveness of existing control mechanisms are assessed, additional risk elimination measures are proposed where necessary, and new potential risks are identified where appropriate. At the same time, we have published Anti-Fraud Policies, established contact addresses for reporting suspected fraud, use available IT tools, provide assistance to law enforcement authorities and other authorized entities, etc.

The Programme Slovakia 2021 – 2027: The programming of the Slovakia Programme was completed at the end of 2022. The implementation of the program did not start in 2022.

The Ministry of Environment of the Slovak Republic, acting as the managing authority for the Operational Programme Quality of Environment 2014 – 2020 (OP QE) stated, that as part of the risk management of the OP QE, recommendations are implemented on an ongoing basis by analysing individual fraud risks in relation to available resources/data in order to identify and address potential risks in a timely manner.

The Supreme Audit Office of the Slovak Republic (SAO SR) has not yet been granted access to ARACHNE, but has requested authorization for its access by the Ministry of Investments, Regional Development and Informatization of the Slovak Republic. Nevertheless, based on legislation and its own monitoring, SAO SR collects necessary information, data and documents for the purposes of risk analysis. Based on the set up strategic focus of its audits, SAO SR is moving forward with its so-called floating planning system, beginning from 2023. Thanks to it, it will be able to include action plans for audits in a more flexible, risk analysis based as well as in a time appropriate manner. The audit plan will be adjusted and expanded during the year based on significance, the results of risk analyses and suggestions from the office's memorandum partners or the public. The new Development Strategy for the years 2023-2025 describes key risks from a financial and property point of view, but also in relation to the obligations of the Slovak Republic towards international organizations, such as the EU or the UN. SAO SR closely cooperates with institutions involved in criminal proceedings (police, prosecution), both when it detects or suspects a crime committed, via notification of detected deficiencies and also carries out audits based on suggestions by the institutions.

Public Procurement Office (PPO) informed, that officials of the Supervision Department carrying out review procedures, and staff of the Public 9

Procurement Department work with public sources in the course of their work for verification and prevention in the detection of conflict of interest in public procurement. PPO has introduced in the internal directive on public procurement the obligation of the staff of the Public Procurement Department that the verifier in charge of public procurement is obliged to use external sources of information in the review of possible conflict of interest, including publicly accessible electronic databases of natural and legal persons (e. g. www.foaf.sk) and other publicly available information. The Supervision Department implements national project funded by the Operational Programme Effective Public Administration "Increasing efficiency in public procurement in Slovakia", which is aimed at unifying decision-making practice and detecting potential conflicts of interest. The Supervision Department on the basis of project implementation developed the Methodology of the Supervision Department, which is backed by a team of six staff members and aims to answer questions from control officials seeking connections between procurement officials and bidders to spot red flags for conflict of interest. Internal methodologist of Supervision Department use access to an online licensing database (Index Podnikatela), which provides information, analyses and reports on legal and natural person entrepreneurs by linking 26 different public databases. In addition to this licence, the internal methodologist of the Supervision Department also use publicly available

resources such as the following to detect potential conflict of interest, the register of end users of benefits, results of municipal and higher territorial unit elections, which also include elected deputies in local government bodies, the register of authorised civil engineers, information published in the media about potential links, the register of non-governmental non-profit organisations maintained by the Ministry of the Interior of the Slovak Republic, the database created by the third sector on major cases in order to navigate through the media and publicly available information (www.kauzy.sk).

The Government Office of the Slovak Republic, acting as the National Implementation and Coordination Authority for the Slovak Recovery and Resilience Plan (RRP) informed that line ministries implementing the RRP have been instructed in order to strengthen the ability to ensure the identification of possible fraud, conflict of interests and corruption when performing checks to use all available verification options and data and information (e.g. publicly available registers, data in the information and monitoring system, ARACHNE information system, social network www.foaf.sk, etc.).

Revenue area:

The responsible departments of the Financial Directorate of the Slovak Republic actively analyse various available data sources (external/internal) also on their own initiative on the basis of the imports development. They identify trends of circumvention of customs regulations. Subsequently there is communication and exchange of relevant information / findings of the respective department within other departments of the Financial Directorate of the Slovak Republic itself, as well as communication of the Financial Directorate of the Slovak Republic with the Criminal Office of the Financial Administration but also with the European Commission, depending on the 10 specific cases. Vice - versa, the European Commission, through its anti-fraud office OLAF, communicates with the respective departments in charge of the Financial Administration of the Slovak Republic, in particular with the Criminal Office of the Financial Administration or with the Financial Directorate of the Slovak Republic regarding detected fraud in order to identify and address in a timely manner emerging risks and trends in customs fraud and to translate them into the prevention of the occurrence of such fraud in a preventive manner. The issue of risk analysis was also discussed by the Financial Directorate of the SR with representatives of the European Commission on 7 October 2022 in Bratislava. In connection with the detection and investigation of customs fraud, the Financial Administration of the SR and the Criminal Office of the Financial Administration cooperate with the European Public Prosecutor's Office as well.